**Appendix I – University of Rochester Human Subject Research Electronic Data Security Assessment Form**

**Principal Investigator:**

**Click IRB STUDY#:**

**Title:**

**Sponsor:**

**Date Completed:**

Investigators must complete this form when data is collected, transmitted, or stored electronically. The information in this form does not need to be specifically repeated in the research protocol, rather the form should be referenced in the protocol and the completed form will be included as part of the new study application in the IRB Review System. On the Ancillary Committee Review Smart form, answer yes to question #1 and then answer all questions appropriately. Question #13 will pertain to the “collection, transmission, or storage of electronic data.” Upload the Data Security Assessment form under “Upload Relevant Documents” and select the Data Security category. If an image is available to describe the lifecycle of the data, please include that in this section, as well. The IRB may request a consultation from data security experts from the University of Rochester Information Security, Academic IT, or HIPAA Privacy to ensure risks to subjects are minimized and appropriate data safeguards are in place. It is possible that these additional data security experts may impose additional requirements, such as a vendor/collaborator qualification questionnaire or an agreement(s). **It is important that all relevant questions are addressed to prevent a delay in review.**

If during the conduct of this research, the responses contained in the form (Appendix I) change (e.g., technologies, data management strategies, data sharing), an updated form must be included in the application of the [IRB Review system](https://rochesterirb.huronresearchsuite.com/IRB/sd/Rooms/DisplayPages/LayoutInitial?Container=com.webridge.entity.Entity%5bOID%5b0A7646F3B149874E902185897C144551%5d%5d) through the modification process. When a revised form is submitted, update the “Date Completed” in the header on the form to indicate that a new version has been completed. Additional information about submitting a modification to the RSRB can be found on page 22 of the [Click® IRB: Study Staff Manual](http://www.rochester.edu/ohsp/documents/education/pdf/ClickIRB_StudyStaffManual.pdf).

* It is important to remember that **research data generated under federal funding belongs to the University of Rochester.**
* All purchase agreements should be processed by the University Purchasing Office.

Questions specific to the Data Assessment Form or IT Security Questionnaire can be made to [Infosec Risk and Compliance](mailto:InfosecRiskandCompliance@UR.Rochester.edu?subject=Question%20About%20Data%20Security%20Assessment%20Form).

|  |  |
| --- | --- |
| **Data Description** | |
| 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 or shared outside the University, 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 | 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  Web Universal Resource Locators (URLs)  Other: |
| 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 (e.g. genomics data)**:** | |
| 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 subject?  Yes  No  Indicate how the coded data will be stored separately from the identifiable data:  Will you be collecting any high risk data?  Yes  No  Data is considered to be high risk when protection of such data is required by law or regulation, protection is necessary in order for the University or its affiliates to meet compliance obligations, or the unauthorized disclosure, access, alteration, loss or destruction of those data could have a material impact on the University or its affiliates’ mission, assets, operations, finances, or reputation, or could pose material harm to individuals. Additional information is available in the University of Rochester [Data Security Classification Policy](https://www.rochester.edu/provost/wp-content/uploads/2020/07/Data-Classifications-Policy-Final-June2020.pdf).  In research specifically, data is high risk when the disclosure of identifying information could have adverse consequences for subjects or damage their financial standing, employability, insurability, or reputation. | |
| Will you collect or receive personally identifiable data or coded data from or about persons physically located in the European Economic Area (EEA)?  Yes  No  *See the* [*European Union’s General Data Protection Regulation (GDPR) Q and A for Researchers*](http://www.rochester.edu/ohsp/documents/ohsp/pdf/policiesAndGuidance/Guideline_for_GDPR_QA_for_researchers_with_graphics.pdf)    If yes, will you be collecting any of the following information?  Racial or Ethnic origin  Trade Union Membership  Political Opinions  Genetic or Biometric Data  Religious or Philosophical Beliefs  Sexual Orientation or information related to sex life | |

|  |
| --- |
| **Part A - Technologies Used to Collect the Data** |
| **Software** |
| |  |  | | --- | --- | |  | Bio-Lab Informatics System (BLIS) / LabKey Server | |  | Biospecimen Inventory Management (BSI) | |  | Box cloud-based file storage (UR Box) | |  | Code42 CrashPlan | |  | Complion: eRegulatory for Clinical Research Sites | |  | eRecord | |  | OnBase: Document Management System (URMC only) | |  | OnCore Clinical Trials Management System (CTMS) | |  | URMC REDCap (Research Electronic Data Capture) | |  | URMC Office 365 OneDrive for Business | |  | Zoom: Video and Web Conferencing  UR  URMC | |  | Other (specify): **- CABIN MRI system (Siemens Syngo)** | |  |  | |
| **Mobile Application(s)** |
| 1. Name of the mobile application: 2. Version of mobile application: 3. Identify the mobile device platform(s) to be used:   iOS  Android  Windows  Other:   1. Identify who created the mobile application: 2. Which device will be used:   University of Rochester owned mobile device  Third party (sponsor, coordinating center, Clinical Research Organization, etc.) owned mobile device  Personal device owned by the subject   1. Will the mobile device be managed with XenMobile?  Yes  No 2. Address how the mobile application is downloaded to the device: 3. Will data be stored on device for any period of time?  Yes  No    1. If yes, please describe (e.g. data queued on device, then transmit to server; data stored on device indefinitely)?    2. Is the data encrypted on device?  Yes  No 4. How is the mobile application secured on the device:     1. Is a password or PIN for the application required?  Yes  No    2. Is a password or PIN for the device required?  Yes  No 5. Will the mobile application be able to access other device functionality such as Location, Contacts, Notifications, etc.? 6. Will identifiers be collected, stored or transmitted from the mobile application?  Yes  No If Yes, ensure all identifiers are checked above under “Data Description.” 7. Where is data transmitted by the device? \*     1. How is it encrypted in transit?   **\* If data is transmitted, contact the** [**Office of Research Project Administration**](https://www.rochester.edu/orpa/) **(ORPA) as an Agreement, and/or Information Security Questionnaire may be required.**   1. How is the data coded?     1. Are phone numbers or mobile identification numbers stored with data:  Yes  No 2. When data is transmitted from the device, please list all locations where it will reside (even temporarily): 3. Provide any additional information: |
| **Wearable Device(s)** |
| **If a mobile application will be used with the wearable device, also complete the mobile application section above.**   1. Name of wearable device: 2. Is wearable device **provided** by subject or research team:   Research team provides device  Personal device used   1. Is wearable device **registered** by subject or research team:   Research team registers device  Subject registers device   1. Will identifiers be collected, stored or transmitted from the wearable device?  Yes  No If Yes, ensure all identifiers are checked above under “Data Description.” 2. Where is data transmitted by wearable device? **\***     1. How is it encrypted in transit?   **\* If data is transmitted, contact the** [**Office of Research Project Administration**](https://www.rochester.edu/orpa/) **(ORPA) as an Agreement, Information Security Questionnaire, and/or Contract may be required.**   1. How is data coded?     1. Are phone numbers or mobile identification numbers stored with data?  Yes  No    2. Will GPS/Location data be collected to identify locations?  Yes  No 2. When data is transmitted from the wearable device, please list all locations where it will reside (even temporarily): 3. Provide any additional information**:** |
| **Electronic/Digital Audio or Video Recordings/Conferencing, Photographs, or Medical Images** |
| 1. Describe the method of capturing the recording, photograph, or image: **MRI** 2. Will the recording, photograph, or image be transmitted over the internet?  Yes  No 3. Will the recording, photograph, or image be accessible to, shared with, or transferred to a third party?    Yes  No  if yes, who will it be transferred to?  How will it be transferred? 4. How will the recording, photograph, or image be secured to protect against unauthorized viewing or recording? **Raw MRI images will ONLY be stored on a HIPAA-compliant password protected server (SMDNAS), access and analysis will be performed by study team. Third parties will only be provided with fully de-identified data (Any DICOM identifiable tags, private tags and skull/facial features stripped)** 5. Provide any additional information**:** |
| **Text Messaging** |
| 1. How will text messages be sent?   University-issued Mobile Device  Third-Party Texting Platform If a third-party texting platform, which one:   1. How will the text messages be received on the mobile device or a separate application?   Current Messaging Application, e.g. messages  Separate Messaging Application\*  **\*** If using a separate messaging application, ensure the mobile application section above is completed.   1. Whose mobile device will be used:  Research team provides device  Subject’s device 2. What is the content of the messaging: 3. Who/What Address will appear in the text as the sender of the message? 4. Can subjects “opt out” of receiving text messages? Yes  No If yes, what is the process/mechanism used to ensure texts are not sent to those who opt out? 5. Will messages be limited to appointment reminders? Yes  No 6. Will messages be limited to survey links? Yes  No 7. Is the communication one-way or two-way: One Way  Two Way 8. Provide any additional information**:** |
| **Other Technologies** |
| 1. Is any other technology being used to collect data? Yes  No   If Yes, describe: |

|  |
| --- |
| **Part B – Data Management** |
| **After Data collection, where will data be processed and stored** |
| 1. **Servers and Storage**   UR/URMC Department Managed Server, indicate which (check all that apply):  Research & Academic IT  URMC ISD  University IT  Department: **Neuroscience - server cluster (DICOM router), XNAT**  UR/URMC Managed Service and Storage, indicate which (check all that apply):  URMC REDCap  SMDNAS Research Storage (SMDNAS)  URMC ISD Shared File Services (ntsdrive)  University IT Shared Files Services  Center for Integrated Research Computing (CIRC)  Other (describe):   1. **Cloud File Storage**   Box cloud-based file storage (UR Box)  URMC SharePoint Online  URMC Office 365 OneDrive  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   UR owned desktop, laptop, or other device  URMC owned desktop, laptop, or other device  Personal desktop, laptop, or other device (**\*** This may violate University Policy.)   1. Will research data be stored on the computer or device Yes  No    1. If yes, what product is used to encrypt data? **Bitlocker/FileVault2**    2. Is antivirus software installed and up to date? Yes  No    3. If yes, what product and version? **Crowdstrike**    4. Is the operating system kept up to date with Microsoft Windows or Mac OS updates? Yes  No 2. Describe the method or mechanism by which data will be transferred from the collection technology to the storage site. SMB file share 3. Provide any additional information: |
| **PART C – Data Analysis and Use** |
| 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? **The PI will review the list of study members and any access control lists yearly and request changes to the access control lists as necessary** 4. Is this an application where UR will be the data coordinating center? Yes  No 5. What technology or software will be used to analyze the data? 6. What data movement is required for this platform to access the data? 7. Where will analytical output be stored? 8. Who has access to the output? 9. Are there any restrictions on who can access the output? 10. Provide any additional information: |
| **Part D. Data Transfer and Final Disposition** |
| 1. Will data be transferred to a third-party collaborator, sponsor, or other party?  Yes**\***   No    1. Third party collaborator, sponsor, or other recipient of research data (identify by name and country of the main office or site where data will be transferred):    2. If yes, is this information identifiable?  Yes  No    3. If yes, will it be transferred outside of the covered entity?  Yes  No    4. If yes, how will it be transferred, and is it encrypted in transit:    5. If yes, what data elements will be transferred? (if there are more than 2 data recipients, please provide a data flow diagram, as a separate attachment) 2. Does the sponsor have requirements for publishing, preserving or destroying the data once the study is complete?  Yes  No    1. If so, what technology will be used for this? **PI will manage data stored on CABIN/Neuroscience servers and indicate when this data should be preserved or destroyed** 3. Describe what will happen to the electronic data when the study is completed and how long research records will be maintained consistent with [University Policy on Retention of University Records](https://www.rochester.edu/adminfinance/records.html#:~:text=Archival%20records%20are%20retained%20and,include%20records%20in%20this%20category.) and [University of Rochester OHSP Policy 901 Investigator Responsibilities](http://www.rochester.edu/ohsp/documents/ohsp/pdf/policiesAndGuidance/Policy_901_Investigator_Responsibilities.pdf):   **\* Contact the** [**Office of Research Project Administration**](https://www.rochester.edu/orpa/) **(ORPA) as an Agreement, Information Security Questionnaire, and/or Contract may be required.** |
| **Please note:** If at any time there is a data breach, you are responsible for submitting a research event to the RSRB, according to [OHSP Policy 801 Reporting Research Events](http://www.rochester.edu/ohsp/documents/ohsp/pdf/policiesAndGuidance/Policy_801_Reporting_Research_Events.pdf) and [Guideline for Reporting Research Events](http://www.rochester.edu/ohsp/documents/ohsp/pdf/policiesAndGuidance/801a_GDL_Reporting_Research_Events.pdf). If an External IRB has reviewed and approved your study, you should report this event to both the external IRB and the RSRB. In addition, suspected breaches of PHI and suspected data security incidents should be reported in accordance with [HIPAA Policy OP31 Breach of Unsecured Protected Health Information](https://sharepoint19.mc.rochester.edu/sites/HIPAA/Privacy/P31.pdf) and [UR/URMC Information Security Incident Management Procedure](https://sharepoint19.mc.rochester.edu/sites/HIPAA/Security/0SEC11Procedure.pdf).  **PI Certification Regarding Terms of Service for Technologies Used for Research Activities**  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.  If yes, provide links to all terms of service:  Name: Date: |