This is a dual department form used by:

* IRB to assist with determinations appropriate for use of electronic study tools (i.e. eConsents, mobile apps)
* IMS to assess institutional safeguards and to assist with purchasing applications/platforms, where necessary.
* If the electronic study tool is used to collect, store, share **non-identifiable** data, **do not complete this form**.

Using this form – To check the checkboxes, double click once on the box. To enter text in the text boxes, click once on the gray box and then type your response.

|  |  |  |  |
| --- | --- | --- | --- |
| **Item 1: What tool (s) are being used?**  *[Select all that apply]* | | Electronic Informed Consent tool (eIC); Provide name of program used and URL (if available):       *[Answer Items 1 – 14 & proceed to Section A]*  Mobile Application (Mobile App); Provide name of Mobile App to be used and URL (if available):      *[Answer Items 1 –14 & proceed to Section B]*  Online Platform; Provide name of platform to be used and URL (if available):       *[Answer Items 1 –14 & proceed to Section B]* | |
| 1. Are there reference materials related to the eIC tool, Mobile App, or Online Platform?   *[Reference materials can be the Protocol or any other documents that provides a description of tool/app, step-by-step screenshots, user agreements, etc.]* | | Yes, Reference Material(s) or URL:  No |

|  |
| --- |
| **Item 2: Does the study have a pending or approved Data Acquisition, Access, Use and Release Request (**[**DAUR) Form**](https://www.uthscsa.edu/sites/default/files/Services/forms/daur-request.docx)**?**  *This form is required for review and approval by the UT Health San Antonio Patient Data Governance Committee (PDGC) when there is new acquisition, access, use or release of sensitive and/or identifiable information associated with external entities outside Treatment-Payment-Operations or under a HIPAA waiver for research protocols.* |
| Yes, study has been approved by PDGC and approved DAUR form is attached *Skip to item 10*  Yes, study is currently under review by PDGC and the approved DAUR form is pending *Skip to item 10*  No *Continue on to Item 3* |

|  |  |
| --- | --- |
| **Item 3: What information will be recorded?**  *[Select all that apply]* | Protected Health Information (PHI) – include the developer in the HIPAA Authorization  Private Identifiable Information (PII) - include the developer in the HIPAA Authorization  Student Identifiable Information (SII) - include the developer in the HIPAA Authorization  Credit Card Data  Sensitive Digital/Proprietary Research Data  Other types of private information; Describe: |

|  |  |
| --- | --- |
| **Item 4: Data Storage Plan** | |
| Where will recorded data be stored? | University Server  Non-University Server  If data will be stored on a non-University server complete the following:   * Describe connection and storage: * In what country is the server located: |

|  |  |  |
| --- | --- | --- |
| **Item 5: Security** | | |
| **Describe the system security**  *(e.g. restricted access, methods to ensure confidentiality after consent obtained, etc.)* | | See attached reference material:      , Section  Other; Describe: |
| The program/Mobile App system:   1. Ensure[s] the confidentiality, integrity and availability of all electronic PHI created, received, maintained or shared; 2. Identif[ies] and protect[s] against reasonably anticipated threats to the security or integrity of the information; 3. Protect[s] against reasonably anticipated, impermissible uses or disclosures; and 4. Ensure[s] compliance with UT Health San Antonio policies.   *(45 C.F.R. § 164.306(a).)* | Check to confirm understanding that the safeguards are followed. |

Complete the IT Security questions for each external data storage system for the entire project.

|  |  |  |  |
| --- | --- | --- | --- |
| *Answer: Yes, No or N/A or indicate the section as Not Applicable* | **External entity’s name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  Not Applicable | **External entity’s name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  Not Applicable | **External entity’s name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  Not Applicable |
| Are access controls in place such as strong password controls, new user setup, terminated user controls, access review procedures, restricted administrative access, and segregation of duties controls? | Yes No N/A | Yes No N/A | Yes No N/A |
| Is role-based access control (RBAC) implemented? (i.e. user access rights are based on assigned roles in the system) | Yes No N/A | Yes No N/A | Yes No N/A |
| Is there a policy that enforces the concept of least privilege (i.e. users only have access to data or systems required for job function)? | Yes No N/A | Yes No N/A | Yes No N/A |
| Is multi-factor authentication implemented for web-based systems with confidential data? (i.e. at least two factors of authentication: something a user **knows** like a pin or password, something a user **has** like a physical mobile device or security token, something the user **is** like a fingerprint or other biometric, etc.) | Yes No N/A | Yes No N/A | Yes No N/A |
| Are audit logs available and reviewed regularly? (i.e. for tracking/monitoring access activity and reviewing abnormal activity) | Yes No N/A | Yes No N/A | Yes No N/A |
| Is data encrypted in transit? (i.e. from system to system; device to device; SSL/TLS) | Yes No N/A | Yes No N/A | Yes No N/A |
| Is data encrypted at rest/in storage (i.e. disk or database encryption)? | Yes No N/A | Yes No N/A | Yes No N/A |
| Are backup copies made according to pre-defined schedules, encrypted, and securely stored? | Yes No N/A | Yes No N/A | Yes No N/A |
| Is patch management in place for systems and applications, including an outlined patching schedule? | Yes No N/A | Yes No N/A | Yes No N/A |
| Are there procedures in place for vulnerability management, including specific remediation timelines for identified vulnerabilities, and a central repository to track remediation? | Yes No N/A | Yes No N/A | Yes No N/A |
| Are there procedures in place for security incident response, including the identification, resolution, and reporting of events? | Yes No N/A | Yes No N/A | Yes No N/A |
| In case of an adverse event, are there business continuity, disaster recovery or crisis management plans in place? | Yes No N/A | Yes No N/A | Yes No N/A |
| Are there physical security controls and policies in place where data is stored? | Yes No N/A | Yes No N/A | Yes No N/A |
| Geographically speaking, is data currently stored and processed in the US? If No, list location(s) outside of the US: | Yes No N/A | Yes No N/A | Yes No N/A |
| Will data be accessed only by the entity’s representatives located in the US? | Yes No N/A | Yes No N/A | Yes No N/A |
| Has there been an external, independent review of the information security and technology environment within the past 12 months? (i.e. ISO 27001, SOC 2, HITRUST, FedRAMP, FISMA, etc.) | Yes No N/A | Yes No N/A | Yes No N/A |
| Has the entity had a significant breach in the last 5 years?  (i.e. compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data that is transmitted, stored or processed) | Yes No N/A | Yes No N/A | Yes No N/A |

**Data Flow Diagram (DFD):** The DFD is a high-level representation of data storage locations and transfers for a project, and should be pasted into the space below. The DFD must include (1) all entities (people, roles, systems, organizations) with access to data, (2) all data storage locations and (3) all transfers between systems. The UTHSA Firewall and all data transfers that cross the UTHSA firewall must be explicitly shown. The DFD must cover all data transfers and storage locations for the entire duration of the project. (*Delete the example included below and replace with your own diagram*.)

|  |
| --- |
|  |

**State any ways in which internal UTHSA systems and external systems will be linked**.

|  |
| --- |
|  |

Or indicate:No Linkage

|  |
| --- |
| **Item 6: Backup procedures -** Describe back-up plans, including the back-up process, schedule, storage, sharing, and recovery. |
| N/A - Backup procedures are listed in the attached reference material:      ; Section:  Describe: |

|  |
| --- |
| **Item 7: UT Health San Antonio Access Management Provisions** - Will users access University data through the mobile application? |
| No  N/A - Access Management is listed in the attached reference material:      ; Section:  Describe in detail how user accounts are provisioned for users who will be accessing University data through the mobile application: |

|  |  |
| --- | --- |
| **Item 8: Will data be shared with 3rd party entities?** *[e.g. developers or for other marketing use - include the developer or other 3rd party entities in the HIPAA Authorization]* | |
|  | Yes - Describe what information is being shared and method used to share the information: |
|  | No |

|  |  |
| --- | --- |
| **Item 9: Security controls to prevent unauthorized 3rd party accessibility** | |
|  | Mobile device protected with a research code number or password |
|  | Data sharing to a server behind (Insert site(s)      ) firewall |
|  | Other |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item 10: General Data Protection Regulation (GDPR) -** Is there a potential for the study to store, collect, control, or process data of individuals currently in a European Union (EU) country?  No – *skip to Item 11*  Yes – Complete the questions below *[Must include GDPR language in consent or have separate GDPR consent in the submission]* | | | | |
| Will explicit consent be obtained before personally identifiable information is received directly from individuals (i.e., they have checked a box indicating their agreement to such data collection)? |  | Yes |  | No |
| Will copies or records of consents be retained? |  | Yes |  | No |
| Will explicit consent be obtained when personal data consists of racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data, biometric data, sexual orientation, trade union membership, criminal convictions or offenses? |  | Yes |  | No |
| If websites related to the study will collect personal information from visitors, will a privacy policy be posted on the website? |  | Yes |  | No |
| Are visitors notified of the way in which their data is used if their personal information is collected from a website? |  | Yes |  | No |
| Is there a process in place to respond to individual requests about amending or deleting personally identifiable data? |  | Yes |  | No |

|  |  |
| --- | --- |
| **Item 11: Will there be a cost to use the eIC or Mobile App?** | No  Yes, *(Include cost of use in the Cost section of the consent form)* |

|  |  |
| --- | --- |
| **Item 12: Does the subject need to download a program or Mobile App*?*** | No  Yes, *(Include download instructions in the Procedures section of the consent form)* |

|  |  |
| --- | --- |
| **Item 13: How will subject questions be addressed** | In person  Videoconference  Phone call  Live chat, please describe data security and privacy protection:  Other, please describe:  See attached reference material:      , Section: |

|  |  |
| --- | --- |
| **Item 14: Describe considerations made for subjects who have impaired vision or motor skills and those who are unfamiliar with working technology.** | Research team guided  Assistance/involvement of family member or caregiver  Audio options available, please describe:  Paper Informed Consent document will be used  Other, please describe: |

|  |
| --- |
| **Item 15: Breach of Confidentiality –**Describe any reasonably foreseeable risk associated with a breach of confidentiality |
| N/A, Risk described in the informed consent document – do not complete this portion.  N/A, No reasonably foreseeable risks associated with a breach of confidentiality  Describe: |

|  |  |
| --- | --- |
| **Item 16: Sponsor and/or Manufacturer contact information** | |
| Sponsor:  Email:       Phone: | Manufacturer:  Email:       Phone: |

**Section A. eInformed Consent – Study is being reviewed by UT Health San Antonio IRB**

N/A – Study is being reviewed by an External IRB, do not complete Section A.

|  |  |  |
| --- | --- | --- |
| **Item A1. Where will the consent process occur?** | | |
| **Is the consent process occurring remotely?** | | No, the process will take place in-person, *continue to Item A2*  Yes*, answer question a. below.* |
| 1. What is the process for authenticating the user? | See attached reference material, Section  Describe: |

|  |  |
| --- | --- |
| **Item A2. What is the process for ensuring that the responses and signatures within the IC cannot be altered?** | Read-Only signature field  Only the subject has ability to change signature  Other: Describe: |

|  |  |
| --- | --- |
| **Item A3. How long will the eIC process take?** |  |

|  |  |
| --- | --- |
| **Item A4. How will signatures be captured?** | Using e-signatures (following guidance in [*FDA Part 11*](https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11&showFR=1&subpartNode=21:1.0.1.1.8.3)*\** for FDA regulated studies)  Other (e.g. checkbox consent), please describe: |

|  |  |
| --- | --- |
| **Item A5. How will subjects receive a copy of the consent form?** | A copy will be emailed to the subject  A copy will be printed for the subject  Other, please describe:  See attached reference material:      , Section  Subject will print/download a copy themselves *(answer a. and b. below)* |

|  |  |
| --- | --- |
| 1. How long will subject have access to the signed e-consent form? (Please disclose in consent form) |  |
| 1. If your study is accessing or collecting protected health information, HIPAA requires that a signed authorization be provided to the subject. | Confirm the understanding that a signed version of the consent form (when the consent form is combined with the HIPAA authorization) will be provided to the subject or subject’s LAR unless the IRB grants an alteration (which excludes HIPAA Authorization signature) or a waiver of the requirement to obtain HIPAA authorization. |

|  |  |
| --- | --- |
| **Item A6. Will the re-consenting of Subjects need to occur?** | No – Rationale:  Yes *(answer a. and b. below)* |

|  |  |
| --- | --- |
| 1. **How will subjects be notified for re-consenting?**   *[Ensure use of most current (IRB-approved) version of consent form, confirm with version date and IRB approval date.]* | See attached reference material:      , Section  Other: |
| 1. **Describe process for re-consenting subjects.**   *[Note: re-consenting of subjects does not need to occur in the same fashion as initial consent.]* | See attached reference material:      , Section  Other: |

**Section B. Mobile App/Online Platform**

(Use the copy and paste function if multiple Mobile Apps/Online Platforms are being used in this study)

|  |  |  |  |
| --- | --- | --- | --- |
| **Item B1. Device Information**  (*Include a copy of applicable reference materials with your IRB application (User agreements, Guides etc.*) | | | |
| **List Application platform(s) (IOS, Android, Windows Mobile)** | | |  |
| Provide the Institution Name of the Mobile App/Online Platform developer. *[Note: If using a commercially available app, you may need to purchase through the UT Health San Antonio purchasing office]* |  | UT Health San Antonio | |
|  | Non- UT Health San Antonio:  *[Note: A data use agreement or contract may be required – contact Office of Sponsored Programs (OSP)]* | |

|  |  |
| --- | --- |
| **Item B2. What is the purpose of the Mobile App/Online Platform?***[e.g., provide subject documentation of adverse events]* |  |

|  |  |
| --- | --- |
| **Item B3. Is the developer designing the Mobile App/Online Platform for the study?** | No  Yes - If yes, this will involve ownership/intellectual property issues that will require additional review - contact Office of Sponsored Programs (OSP). |