***Items in blue italics are for appropriate office use only***

**Request/Project Title**:

|  |
| --- |
|  |

**Requestor/PI:**

|  |
| --- |
|  |

**Requester’s Department**:

**Initial Request Date** (dd-Mon-yyyy):       -       -

**Date by which a decision is needed;** Indicates urgency. (dd-Mon-yyyy):       -       -

**Planned project start date** (dd-Mon-yyyy):       -       -

**Planned project end date** (dd-Mon-yyyy):       -       -

**Project classification(**select one)**:** [ ] TPO [ ] Research [ ] Infrastructure

**Indicate any of the following required by the request**

Acquisition of a data source new to UTHSA [ ] Yes [ ] No

External release of data [ ] Yes [ ] No

New internal movement or storage location of data [ ] Yes [ ] No

New use of existing Epic access [ ] Yes [ ] No

New Epic access necessary [ ] Yes [ ] No

 If Yes, describe

|  |
| --- |
|  |

**UTHSA Providing Data( cc:** **grc@uthscsa.edu****)** [ ]  **UTHSA Receiving Data** [ ]

**IRB status**: [ ]  Not Applicable

[ ]  IRB human subjects protocol [ ] planned, [ ]  in-process, [ ]  approved (HSC IRB#      )

[ ]  IRB protocol amendment [ ] planned, [ ]  in-process, [ ]  approved (HSC IRB#      )

[ ]  IRB exempt determination [ ] planned, [ ]  in-process, [ ]  approved (HSC IRB#      )

[ ] Non-research determination [ ] planned, [ ]  in-process, [ ]  approved (HSC IRB#      )

[ ] Non-human determination [ ] planned, [ ]  in-process, [ ]  approved (HSC IRB#      )

***IRB Verified*** [ ] *Yes* [ ]  *No*

|  |
| --- |
| *Additional information / Comments* |

**PHI Authorization Status (check all that apply)**: [ ]  Not Applicable

[ ] HIPAA Authorization: [ ] planned, [ ]  in-process, [ ]  executed

[ ] HIPAA Waiver: [ ] planned, [ ]  in-process, [ ]  executed

***IRB Verified*** [ ] *Yes* [ ]  *No*

|  |
| --- |
| *Additional information / Comments* |

**Funded projects (check all that apply)** [ ]  Not Applicable

[ ] Associated Grant/Project ID#

[ ] Data originally obtained from a repository/catalog, or source other than UTHSA

*(Describe and name source       )*

***OSP Verified*** [ ] *Yes* [ ]  *No*

|  |
| --- |
| *Additional information / Comments* |

**Agreement Status (check all that apply)**: [ ]  Not Applicable

[ ] Data Use Agreement: [ ] planned, [ ]  in-process, [ ]  executed

[ ] Contract / agreement: [ ] planned, [ ]  in-process, [ ]  executed

***OSP Verified*** [ ] *Yes* [ ]  *No*

|  |
| --- |
| *Additional information / Comments* |

**IP Disclosures (check all that apply)** *(Intellectual property or invention disclosures are associated with the transferring data)***:** [ ]  Not Applicable

[ ] Investigator is leaving the institution [ ]  Yes [ ]  No

[ ] Type of data leaving the institution [ ]  Original data [ ]  Copy of data

***Export Controls Verified*** [ ] *Yes* [ ]  *No*

|  |
| --- |
| *Additional information / Comments* |

**Request Category** (check all that apply):

[ ] Data acquisition: [ ]  Identified1 [ ]  Sensitive2 [ ]  LDS3 [ ]  De-identified4 [ ]  In public domain

[ ] Data access: [ ]  Identified1 [ ]  Sensitive2 [ ]  LDS3 [ ]  De-identified4 [ ]  In public domain

[ ] Data use: [ ]  Identified1 [ ]  Sensitive2 [ ]  LDS3 [ ]  De-identified4 [ ]  In public domain

[ ] Data release: [ ]  Identified1 [ ]  Sensitive2 [ ]  LDS3 [ ]  De-identified4 [ ]  In public domain

|  |
| --- |
| Additional information / Comments |

1Identified is defined by the 18 HIPAA Identifiers include: (1) Name (including initials); (2) Address (all geographic subdivisions smaller than state: street address, city, county, zip code); (3) All elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age if over 89); (4) Telephone numbers; (5) Fax number; (6) Email address; (7) Social Security Number; (8) Medical record number; (9) Health plan beneficiary number; (10) Account number; (11) Certificate or license number; (12) Any vehicle identifiers, including license plate; (13) Device identifiers and serial numbers; (14) Web URL; (15) Internet Protocol (IP) Address; (16) Finger or voice print; (17) Photographic image - Photographic images are not limited to images of the face; (18) Any other characteristic that could uniquely identify the individual

2 Sensitive data includes confidential / high risk personnel or research data

3 A Limited Dataset must omit all of the HIPAA identifiers except for the following: 1. City, state, zip code; 2. Dates of admission, discharge, service, date of birth, date of death; 3. Ages in years, months or days or hours

4 In order to be considered “de-identified” all 18 HIPAA Identifiers for Personally Identifiable Information (PII) or Protected Health Information (PHI)\* must be removed with the following additional caveats: 1. All geographic subdivisions smaller than a state, except for the initial three digits of the ZIP code: (i) The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and (ii) The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000; 2. Ages in years and for those older than 89, all ages must be aggregated into a single category of 90 or older.

**Requester Attestation of Compliance**:

[ ] I have reviewed the above and attest the classifications marked meet the applicable definitions.

**Indicate any of the following that are included in the request: (**Defined in HOP 5.8.21)

Confidential/high risk data – Protected Health Information (PHI) [ ] Yes [ ] No

Confidential/high risk data – Student Identifiable Information [ ] Yes [ ] No

Confidential/high risk data – UT Health Personnel Information [ ] Yes [ ] No

Confidential/high risk data – Sensitive Digital Research Data [ ] Yes [ ] No

Confidential/high risk data – Other Sensitive Information [ ] Yes [ ] No

Controlled data (not available to the public) [ ] Yes [ ] No

Published data (available to the public) [ ] Yes [ ] No

Financial account of credit card account information of individuals [ ] Yes [ ] No

Social Security Numbers [ ] Yes [ ] No

Provide details if “Yes” is checked in any of the above:

|  |
| --- |
|  |

**Statement of how Minimum Necessary will be met and maintained:**

|  |
| --- |
|  |

**Data Release:** [ ]  Not Applicable

|  |
| --- |
| *Mark all entities that may have access to research data and/or specimens****either viewed on site or transferred.*** |
| **Entity Role***(select all applicable)* | For each entity, **select all applicable** |
|  | **Identifiable materials** | [**Limited Data Set**](http://privacyruleandresearch.nih.gov/dictionary.asp#l)(i.e. may include elements of dates, city, state, zip) | **Non-identifiable materials** | **Describe how the materials will be viewed and/or transferred (*If using eCRF, provide website. Note -those entities receiving identifiable information or a limited data set must also be listed on the HIPAA authorization or waiver*** |
|  | **Viewed** | **Transferred** | **Viewed** | **Transferred** | **Viewed** | **Transferred** |  |
|[ ]  Sponsor and/or CRO |[ ] [ ] [ ] [ ] [ ] [ ]  Method for viewing:       Method for transferring:        |
|[ ]  Monitor |[ ] [ ] [ ] [ ] [ ] [ ]  Method for viewing:       Method for transferring:        |
|[ ]  Coordinating Center |[ ] [ ] [ ] [ ] [ ] [ ]  Method for viewing:       Method for transferring:        |
|[ ]  Other sites, investigators or collaborators participating in this study. *Specify(include names and contact information*):          |[ ] [ ] [ ] [ ] [ ] [ ]  Method for viewing:       Method for transferring:        |
|[ ]  Others not participating in this study.*Specify(include names and contact information*):          |[ ] [ ] [ ] [ ] [ ] [ ]  Method for viewing:       Method for transferring:        |
|  |  |  |  |  |  |  |  |  |  |

**Data Storage Media and Access Controls:**

[ ] Paper

 [ ] Informed Consent Forms, [ ] Documents, [ ] Structured data

 Describe how the data will be secured and who has physical access.

|  |
| --- |
|  |

[ ] Electronic data

 List data storage systems for entire projectbefore and after planned data release. List software applications used for the project and where the software is installed. Classify systems as **internal UTHSA data storage** such as an institution workstation, department server in the UTHSA network, **or** **External Data Storage**, i.e., Non-**UTHSA** server, such a vendor’s system or a collaborator’s system at another institution. For External Data Storage, state whether the Office of Information Security has completed a risk assessment for the software.

|  |  |
| --- | --- |
| UTHSA Data Storage: [ ] Epic[ ] REDCap (see[*REDCap User agreement*](http://deb.uthscsa.edu/files/REDCap_End_User_Agreement.pdf))[ ] IDEAS[ ] VELOS eResearch[ ] Clinical Data Warehouse [ ] XNAT[ ] Mobile phones/tablets       [ ] Medical devices       [ ] Consumer/commercial devices       [ ] Departmental server       [ ] Transportable media (CD’s, zip drives, etc.)       [ ] Others  list systems below.                | External Data Storage:Institution: System      :       *For data stored externally, complete, and submit with this DAUR form, a Vendor 3rd Party Risk assessment in the form of a Higher Education Community Vendor Assessment Toolkit (HECVAT) for all Non-UTHSA data storage locations.* Number of HECVAT forms accompanying this request:       |
| Indicate if any of the above will be utilized to obtain informed consent       |
| Provide any 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.* *or URL:*       |
| **State any ways in which internal UTHSA systems and external systems will be linked**.

|  |
| --- |
|  |

 Or indicate:[ ] No Linkage |

[ ] Films

 Please describe:

 Describe how the data will be secured and who has physical access.

|  |
| --- |
|  |

**List Internal and External Data Steward/s for Requested data (**Role and Name of person responsible for the data during the period of use**):**

|  |  |
| --- | --- |
| [ ] N/A: no internal data stewards                | [ ] N/A: no external data stewards                |
| For each new data source describe terms of our use of the data       |

**In addition to the data steward/s List anyone accessing or handling the Requested data (**Role and Name of each person accessing or handling the data during the period of use**):**

|  |  |
| --- | --- |
| [ ] N/A: no internal people accessing data                | [ ] N/A: no external people accessing data                |

**Will any External data stewards accessing or handling the requested data:**

Require an account within the institution's domain (@uthscsa.edu)? [ ] Yes [ ] No

Need remote access to the institution's network or systems? [ ] Yes [ ] No

**IT Security:**

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

(If there is more than one Non-UTHSA data storage location, see Appendix A.)

|  |  |  |
| --- | --- | --- |
| *Answer: Yes, No or N/A or indicate the section as Not Applicable* | **Internal: UTHSA**[ ]  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 |
| 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 |
| 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 |
| 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 mobile device or security token, something the user **is** like a fingerprint or other biometric, etc.) | [ ] 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 |
| Is data encrypted in transit? (i.e. from system to system; device to device; SSL/TLS) | [ ] 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 |
| Are backup copies made according to pre-defined schedules, encrypted, and securely stored? | [ ] 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 |
| 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 |
| 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 |
| 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 |
| Are there physical security controls and policies in place where data is stored? | [ ] 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 |
| Will data be accessed only by the entity’s representatives located in the US?  | [ ] 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 |
| 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 |

***Info Security Verified*** [ ] *Yes* [ ]  *No*

|  |
| --- |
| *Additional information / Comments* |

**Describe (1) the goal of the project and (2) what will be done with the data to meet the goal/s of the project**.

|  |
| --- |
|  |

**Relationship to prior projects / requests:**

|  |
| --- |
|  |

**Data Source Systems** (Data Elements\* from each and look back timeframe must be enumerated)**:**

|  |
| --- |
|  |

\*If notes or reports, need to describe information to be extracted.

**State any ways in which the requested data will be linked or combined with other data**. Directly address increased likelihood of re-identification of de-identified data attributable to the proposed linkage.

|  |
| --- |
|  |

 Or indicate:[ ] No Linkage

**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*.)

|  |
| --- |
|  |

**Workflow Diagram (WFD):** The WFD is a high-level representation of major process steps in data acquisition, access, use and disposal for a project, their sequence and control. Entities performing the operations may be, but is not required, shown in a “swim-lane” format. All major operations on data must be shown on the WFD including Extract-Transform-Load (ETL) procedures, data processing, and measures to protect privacy and confidentiality such as tokenization or encryption. *If steps are sequential and lacking multiple if-then conditions, a list of steps will suffice*.

|  |
| --- |
|  |

**Risk Assessment**

**Indicate the highest risk data involved in the request**: [ ]  Confidential [ ]  Controlled [ ]  Published

**Number of Patients for whom data are involved**: **(**Min – Max**)**:       -

Explanation (if needed):

|  |
| --- |
|  |

**Impact Assessment**:

State the impact of threats to Confidentiality, Integrity, and Availability of the data involved in the request. Rated each as Very Low, Low, Moderate, High, Very High.

**Impact Rating**

Describe the Impact on the **institution** should there be a breach of accessed

or collected data.

|  |
| --- |
|  |

Describe the Impact on the **institution** should the accessed data were corrupted,

adultered, or later found to be inaccurate during or after project conclusion.

|  |
| --- |
|  |

Describe the Impact on the **institution** should the data become unusable

or unavailable for a period of time during or after project conclusion or

completely lost.

|  |
| --- |
|  |

**Likelihood Assessment**:

State the likelihood of threats to Confidentiality, Integrity, and Availability of the data involved in the request. Rated each as Very Low, Low, Moderate, High, Very High.

**Likelihood Rating**

Describe the likelihood of a breach

|  |
| --- |
|  |

Describe the likelihood of the data being corrupted, adultered or found

inaccurate during or after project conclusion.

|  |
| --- |
|  |

Describe the likelihood of the data becoming unusable or unavailable

for a period of time or completely lost.

|  |
| --- |
|  |

**Assign an overall Risk according to the Likelihood versus Impact matrix below**.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Likelihood** | **Impact** | **Risk Level** | *Overall risk is assigned as the highest rating* |
| Loss of Confidentiality |  |  |  |
| Loss of Integrity |  |  |  |
| Loss of Availability |  |  |  |
| **Overall Risk** (Very Low, Low, Moderate, High, Very High): |  |



**Describe the prevention or mitigation strategies for the drivers of moderate and high risk ratings that the requestor commits to implement.**

** Or Indicate** [ ] Not Applicable, No Moderate or High Risks

|  |
| --- |
|  |

**Start date of data use or retention period** (dd-Mon-yyyy):       -       -

**End date of data use or retention period** (dd-Mon-yyyy):       -       -

**Date for data disposal** (dd-Mon-yyyy):       -       -

**Describe the data disposal plan**. *(Indicate if data will not be destroyed, but will be returned to UTHSA)*

|  |
| --- |
|  |

**Is there a cost associated with the data transfer or acquisition:** [ ]  No [ ]  Yes

|  |
| --- |
| *If Yes, provide rationale, calculation of costs, and quote* |

**Estimated Time to Complete this Form:**       Hours

**Requester Attestation of Department Approval**:

[ ] The appropriate individual in my department is aware of this project or work and approves with my undertaking this project or work.

**Requester Attestation of Compliance**:

[ ] The work described in this request will be overseen by me. I will comply with all applicable laws and regulations and the statements made in this application.

**Requestor**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Date** (dd-Mon-yyyy):       -       -

 Signature

***Initial Patient Data Governance Sub-committee review*** *(dd-Mon-yyyy):       -       -*

***Approved by vote of the PDGS-c\**** *(dd-Mon-yyyy):       /       /*

 *\* Modifications, caveats and implementation notes from PDGS-c will be noted in red on approved version. Approved version should correspond to PDGS-c data on which the request was approved or denied.*

***Appendix A***

**IT Security: Non-UTHSA data storage locations**

|  |  |  |  |
| --- | --- | --- | --- |
| *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 |