A Data Risk Assessment addresses security, privacy, and legal risks posed to the University. A Data Risk Assessment is required for Stanford projects that involve any of the following:

* High Risk or Moderate Risk Data
* Use of solutions other than [Stanford Approved Services](file:///C%3A%5CUsers%5Cpparsi%5CAppData%5CLocal%5CBox%5CBox%20Edit%5CDocuments%5C37048566526%5Cdataclass.stanford.edu)
* Involvement of a new entity that will handle Moderate or High Risk Stanford Data

HOW TO INITIATE A DATA RISK ASSESSMENT:



1. Review the [**Stanford Risk Classifications**](https://itservices.stanford.edu/guide/riskclassifications) and the [**Data Risk Assessment process**](https://uit.stanford.edu/security/jsplr) before completing the intake form.
2. Complete the intake form as follows:
	* Sections A and B must be completed by a Stanford individual who has full programmatic knowledge of the project. Questions about these sections should be sent to privacy@stanford.edu.
	* Section C will require consultation with information security and the technical staff involved in the project who will administer the systems. This section may require detailed technical information from your outside collaborator(s). ***Provide the form to them as soon as possible to allow sufficient time for completion.*** Questions about this section should be sent to iso-consulting@lists.stanford.edu.
	* Completely answer ALL questions and specify “N/A” if a question does not apply to your project. Leaving any questions unanswered may delay the review process.



1. Once your intake form is completed and you have gathered all supporting documents, file a ServiceNow ticket as follows:
	* Log into stanford.service-now.com and select ‘Information Technology’.
	* Select ‘Request Something’, category “Security and Compliance,” and Request Type ‘Privacy and Security Review – General Request’.
2. Attach your completed intake form, data flow diagram, related agreements and, if applicable, your IRB application to the ServiceNow ticket. ***Review may be delayed if these documents are not attached. An application is considered complete only when the form is complete and all documents are attached.***

AFTER YOU SUBMIT YOUR COMPLETED APPLICATION:

After receiving your intake form and all supporting documents, your information will be reviewed. If more information or clarification is needed, your technical and programmatic staff and those of your collaborator(s) may be scheduled for a meeting. A report will be issued with recommendations for addressing the risks posed by the project.

QUESTIONS:

General questions about the form or process can be directed to privacy@stanford.edu. Thank you, and we look forward to collaborating with you on this project.

|  |
| --- |
| **STANFORD APPLICANT** |
| SUBMITTER NAME AND TITLEBenjamin Pierce, Associate Professor |
| **IF NOT SAME AS ABOVE,** PROJECT LEAD NAME AND TITLE |
| DEPARTMENTTrauma |
| PHONE NUMBER650-555-5555 | EMAILMASH@stanford.edu |
| PROJECT TITLEAnalysis of the efficacy of wearables in treatment of traumatic brain injury |
| TYPE OF PROJECT[ ]  Medical/Clinical Care [ ]  Student education [ ]  Quality improvement/assessment[x] Research [ ]  Fundraising/marketing [ ]  University administration/operations[ ]  Outsourcing (process, application/service) [ ]  Other (describe): |
| IRB PROTOCOL NUMBER (if applicable) 99999 |

**Please review Stanford’s** [**Risk Classification Guide**](https://itservices.stanford.edu/guide/riskclassifications) **before answering the next portion.**

1. **INFORMATION ABOUT THE PROJECT**
2. **Overview.**
3. Identify all **non-Stanford** parties involved in the project.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Third party/Organization name** | **Role** (e.g., vendor, funding sponsor, business associate, subcontractor, collaborator, technical support, etc.) | **Point of Contact** | [**Moderate Risk Data**](https://uit.stanford.edu/guide/riskclassifications)will be transferred to/ received from / accessed by entity | [**High Risk Data**](https://uit.stanford.edu/guide/riskclassifications)will be transferred to/ received from / accessed by entity |
| MyBrain LLC | Collaborator, device provider | MyBrain LLC, BJ Hunnicutt 301-555-5555, bjh@mybrain.com | No | Yes |
| Gray Matter Inc. | Sponsor | Francis Mulcahy, 410-555-5555, father@ctc.com; sponsor  | No | No |
| Palo Alto VA | Collaborator | Margaret Houlihan, 443-555-5555, maj.marge@va.gov | No | No |

There are also 17 other sites (mostly hospitals and universities) across the US and internationally that will be contributing to the database.

1. In layperson’s language, briefly summarize the overall project, including what each organization/third party identified above will do in the project.

In this study, we will be comparing outcomes of patients with TBIs. One group will wear a device on their wrist, which will monitor their activity and signs and will provide feedback, reminders, and notices to the patient via the device’s app and text messages. The other group will receive standard follow-ups from the study team and will be monitored during regular in-person visits.

Gray Matter is providing funding for this project and is compiling de-identified and aggregated data from all sites to establish an online database.

We are working with the Palo Alto VA to recruit patients from the VA. They are collaborating in the study and will have access to their own patients and their data. They will not have access to Stanford patients or research subjects who are not VA patients.

MyBrain LLC owns the MyBrain device and app; MyBrain will have access to High Risk data of the patients.

Other sites will not be accessing any Stanford data, and Stanford will not be accessing any of their data.

1. What is the target start date for this project or this project phase?

January 1, 2017

1. Is this a new project or an enhancement/adjustment to an existing project?

[x] New [ ] Enhancement/Adjustment

 If enhancement/adjustment, what is being changed?

 [ ] Technology [ ] Vendor [ ] Data [ ] Other (specify):

1. **Project Funding.**  If this project is externally funded, provide the sponsor name, SPO number, or agreement.

Sponsor Name: Gray Matter Inc.

SPO/Agreement #: SPO 1111111

[ ]  Project is not externally funded

1. **Contracts and Other Obligations.** Identify ***and attach*** to your ServiceNow ticket any agreements, obligations or regulatory requirements related to this project, this dataset, or the third parties involved.

[ ]  No known obligations [ ]  Master Agreement

[ ]  Non-disclosure/Confidentiality Agreement [ ]  Umbrella Agreement

[x]  Sponsored Research Agreement [ ]  Business Associate Agreement (BAA)

[ ]  Collaborative Agreement [ ]  Data Use Agreement

[ ]  FIPS, FISMA, NIST requirements in contract [ ]  Other (explain):

1. **Other Involved/Interested Stanford Entities.** Identify any other Stanford entity with whom you have worked or consulted as part of this project.

[ ]  Office of General Counsel (OGC) [ ]  Procurement [ ]  Office of Sponsored Research (OSR)

[ ]  Office of Technology Licensing (OTL) [ ]  Office of Development [ ]  Office of Risk Management

[x]  Industrial Contracts Office (ICO) [ ]  Registrar [ ]  SoM Information Resources & Technology

[ ]  Global Services/International Affairs [ ]  Stanford Hospital/Clinic [x]  Institutional Review Board (IRB)

[ ]  Other Stanford schools or units:

Provide the point(s) of contact for the office(s) selected above.

ICO: Radar O’Reilly, contract officer

IRB: Frank Burns, IRB panel manager

1. **INFORMATION ABOUT THE DATA INVOLVED IN PROJECT**
2. **Data Owner is:** [ ] Stanford [x] Stanford Hospital/Clinic [x]  Other (specify): ­­­­VA
3. a) **Will Non-Stanford parties access Stanford Data?** [x] Yes [ ] No

IF yes, how?

[ ]  Paper [ ]  Thumb-drive/hard drive

[x]  Web portal / Server access (non-SUNet credentials) [ ] View-only

[ ]  Web portal / Server access (sponsored SUNet credentials) [ ]  Download

[ ]  Other:

b) **Will Stanford individuals access non-Stanford data?** [ ] Yes [x] No

IF yes, how?

[ ]  Paper [ ]  Thumb-drive/hard drive

[ ]  Web portal / Server access (non-SUNet credentials) [ ] View-only

[ ]  Web portal / Server access (SUNet credentials) [ ]  Download

[ ]  Other:

1. **Data Elements involved in any part of the project**. Select all that apply and explain, where necessary. Attach a data dictionary, if available.

[ ] Full names (students, alumni)

[ ] Full names (patients, research subjects)

[ ] Full names (employees)

[ ] Full names (all others)

[x] Geographic subdivisions smaller than a state

[x] Dates (except year) directly related to an individual

[x] Telephone numbers

[ ] Fax numbers

[x] E-mail addresses

[ ] Social Security numbers

[ ] Medical record numbers

[ ] Health plan beneficiary numbers

[ ] Account numbers (e.g., medical or insurance)

[ ] Certificate/license numbers

[ ] Vehicle identifiers and serial numbers, including license plate numbers

[x] Device identifiers and serial numbers

[ ] Web URLs

[x] IP address numbers

[ ] Biometric identifiers, including finger and voice prints

[ ] Full face photographic images and any comparable images

[ ]  Other photographic images, video or audio

[ ]  Stanford ID number (student, employee)

[ ] Lab or pathology test results

[ ] Diagnoses or procedures

[ ] Psychology or mental health information

[x] Clinical records

[x] Prescriptions or medications

[ ] Images or radiology reports

[ ]  Passport or Visa numbers

[ ] Employee personnel files

[ ]  Grades or performance (students, alumni)

[ ]  Disciplinary actions or proceedings (students, alumni)

[x]  Demographics (age, sex, etc.)

[ ]  Financial account numbers (e.g., bank accounts, credit)

[ ] Financial records, including credit card or bank information

[ ] Donor contact and gift information

[ ] Salary information

[ ] Employment benefits

[x] Other health, medical or physical or mental status information (describe): appointments; therapy regimen/exercises

[ ] Any other unique identifying numbers, characteristic, or code (describe):

[ ] Other:

1. **Population Size.** Provide an estimate of the number of individuals whose data will be involved in this project.

[x]  1-500 [ ]  501 – 10,000 [ ]  > 10,000

1. **Data is Sourced from** (select all that apply):

[x] STRIDE [ ] Epic or hospital medical records**\*** [ ] Oracle Financials

[ ] Registrar [ ] HR records [x] Participant provided (e.g., surveys, mobile apps) [ ] Government records/systems [ ]  Stanford email or other technical system

[ ] Other non-Stanford system, database, or party

[ ] Other (describe):

\*If you selected Epic or hospital medical records, permission from hospital Privacy Office may be required

1. **Is the data coming into or going out of the United States?** [x] No [ ] Yes (where?):
2. **data is:**

[x] Identifiable [ ]  A limited data set

[ ]  De-identified using the HIPAA Safe Harbor Method [ ]  De-identified using the HIPAA expert determination method

 (if expert opinion, **attach** the written opinion to SNOW ticket)

[x]  Not PHI but de-identified, pseudonymized, anonymized, or otherwise masked as described

**REQUIRED:** If data is not identifiable, describe the process for removal of identifiers.

The information MyBrain gathers is identifiable.

Identifiable information is stored in RedCap. We will then de-identify the information before uploading into Gray Matter’s web portal. A research coordinator will be responsible for removing all 18 HIPAA identifiers before downloading the information from RedCap. All identifiable fields in RedCap are marked as “identifiers: yes” so that they will be automatically excluded from any data pull from RedCap. In addition, the coordinator will double-check the pulled data for any identifiers to confirm that identifiers are not included.

Gray Matter also does a quality assessment of all data, and as part of that review, they ensure there are no identifiers from any of the sites before making the database public.

1. **FOR VENDOR OR TECHNICAL/SECURITY STAFF TO COMPLETE: INFORMATION ABOUT ADMINISTRATIVE SAFEGUARDS, APPLICATIONS, SYSTEMS, and DATA FLOW OUTSIDE STANFORD**
2. **Name and Contact information for Third Party’s Privacy Officer:**

Name**:**

CPO: Max Klinger, mkling@mybrain.com

443-555-5555

Contact Number:

1. **Name and Contact information for Third Party’s Security Officer:**

Name**:**

CISO: Trapper John, trap@mybrain.com

310-555-5555

Contact Number:

1. **Audits, Certifications, and Attestations.**

Please specify **and attach** the most recent annual third party audit report, certification, or attestation covering privacy, security and IT operations and processes, including risk assessment and risk management process; data collection, use, disclosure, storage and destruction policies; software development life cycle; breach/Incident response process; privacy and security awareness training for anyone who handles data; and contingency plan for data recovery in case of an emergency.

[ ]  Soc 1, Type 2 [ ]  HITRUST [ ]  PCI DSS [ ]  ISO 27001/27002 [ ]  NIST 800-53

[x]  Soc 2, Type 2 [ ]  FEDRAMP [ ]  None (**If None**, please attach Privacy Policy and Information Security Policy)

[ ]  Other (describe below)

Report covering October 2015-September 2016 is attached. A bridge letter covering the time from Sept. 2016 until today is also attached.

1. **Application Authentication.**
2. Provide the application URL in support of this project, if applicable.

Project URL: Stanford.mybrain.com

1. Does web portal support Security Assertion Markup Language (SAML)? [ ]  Yes [x]  No

**If no,**

1. Does it support two-step authentication? [x]  Yes [ ] No
2. What are the password complexity requirements (e.g., minimum 8 characters, alphanumeric, etc)?

Minimum 8 characters and at least one upper character, one number, and one special character.

1. **Hosting Environment.** Identify the hosting environment (e.g. Amazon Web Services, physical data center, etc.), backup environment and geographical location of each.

Azure

1. **Data Flow.**
2. **Diagram and System Components.** Attach a diagram(s) depicting the proposed data flow in detail. Diagram should include details, such as protocols, ports, and of each system component. Indicate any connections in which the system may exchange [Moderate Risk](https://itservices.stanford.edu/guide/riskclassifications) and/or [High Risk](https://itservices.stanford.edu/guide/riskclassifications) information with another system.



1. **Storage, Retention and Destruction.** Provide a data flow description for each stage of the data lifecycle (collection, storage, use, transmission, access, and destruction).

Once participants are enrolled, they will be given a MyBrain device to wear on their wrist. They are asked to download the MyBrain app onto their phone or other mobile device. The patient will register and create a “profile” using their email address. The app will then sync with the bracelet and begin recording movement, speed, pulse rate, sweat, temperature, geo-location, etc. We will enter into the app all of their rehabilitation appointments and reminders for any therapeutic exercises that the patient will do on their own. The app will then display a notification on the individual’s phone and send a vibration reminder to the device.

The data is saved in the MyBrain app indefinitely and pushed to the study team nightly. The team will store the data in RedCap. We will remove the names, phone numbers, email addresses, geolocation, and IP addresses from the data, and send the information to the sponsor via their website portal. The sponsor’s database will be available publicly indefinitely.

MyBrain retains all of the data indefinitely to conduct research, surveys, and improve its app and services. They may combine this data with data from other sources to better market their products to their users.

MyBrain platform is hosted in Azure, therefore data is sent to our Azure instance which is geographically located in the US and data is stored in Azure instance. Data is then accessed by our research team via dedicated machines to conduct research and data mining. MyBrain has no intention of destroying data.

Administrative safeguards include dedicated admin and user workstations, account management, two step authentication, logging an monitoring for both users and administrators. See more details in MyBrain’s SOC 2 Type 2 report.

1. **Data in Transit.**
2. What protocols are supported and enabled to transmit application encrypted data? Select all that apply.

[ ] TLS 1.1 [x] TLS 1.2 [ ] Other (specify):

1. Is Stanford initiating the transmission? [ ]  Yes [ ] No
2. Is Stanford pushing or pulling data from other vendor systems? [ ] Pushing [ ] Pulling [ ] Both
3. **Data at Rest**
4. Is data encrypted at rest? [ ]  Yes [x]  No
5. Are backups encrypted? [x]  Yes [ ]  No
6. Describe how encryption keys are being secured, including who has access to the keys.

MyBrain leverages Azure’s Key Management Service to secure encryption keys for data in motion encryption.

1. **Access.**
2. **Users and Administrators.** Identify the individuals, or classes of individuals, and their roles who will have administrator access and who will have user access to the system. Specify who manages access.

MyBrain’s Azure administrators and developers have admin access to the instance for Azure management, configuration and deployment purpose.

All other users, such as MyBrain data scientists and researchers have only limited user access needed for their job function.

Access is managed by MyBrain’s system admins.

1. **User Methods.** Check the different methods by which the users can access the system

 [ ] SSH [x] Web Application [ ] Client Application

 [ ] Other (specify)

Users will be accessing Azure instance using dedicated workstations and Azure login methods, such as username/password with two-factor authentication.

1. **Admin Methods.** Check the different methods by which the administrators can access the system

 [x] SSH [x] Web Application [ ] Client Application

 [ ] Other (specify)

MyBrain’s Azure administrators and developers have admin access to the instance for Azure management, configuration and deployment purpose.