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 Data
* Moderate Risk Data involving 500 or more records
* 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 ‘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** |
| NAME AND TITLE |
| DEPARTMENT |
| PHONE NUMBER | EMAIL |
| PROJECT TITLE |
| TYPE OF PROJECT[ ]  Medical/Clinical Care [ ]  Student education [ ]  Quality improvement/assessment[ ] Research [ ]  Fundraising/marketing [ ]  University administration/operations[ ]  Outsourcing (process, application/service) [ ]  Other (describe): |
| IRB PROTOCOL NUMBER (if applicable)  |

**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. Briefly describe the overall project.
4. Identify all non-Stanford parties involved in the project. Specify 1) name and contact information, and 2) the nature of involvement, such as vendor, funding sponsor, business associate, subcontractor, collaborator, or technical support.
5. For all entities identified in (b) above, describe their role or contribution to the overall project mission, and indicate if any Moderate or High Risk Data will be transferred to or accessed by the third party.
6. What is the target start date for this project or this project phase?
7. **Population and Project Size.** Describe the population (e.g., Stanford Hospital patients, clinical research participants, students, etc.) and provide an estimate of the number of persons for whom the data will be accessed, stored, transmitted, or released.
8. **Project Funding.**  If this project is externally funded, provide the sponsor name, SPO number, or agreement.

[ ]  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. **NOTE:** If you do not have an agreement, you are likely bound by the third party’s terms of service or terms of use, typically found on its website. Please review and **attach** the third party’s terms of service/use and privacy policy.

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

[ ]  Umbrella Agreement [ ]  Sponsored Research Agreement: SPO

[ ]  Business Associate Agreement (BAA) [ ]  Collaborative Agreement

[ ]  Data Use Agreement [ ]  FIPS, FISMA, NIST requirements in contract

[ ]  No known obligations [ ]  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

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

[ ]  Global Services/International Affairs [ ]  SHC/LPCH: [ ]  Institutional Review Board (IRB)

[ ]  Other:

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

1. **INFORMATION ABOUT THE DATA INVOLVED IN PROJECT**
2. **Data is:** [ ]  Incoming [ ]  Outgoing
3. **Data Owner is:** [ ] Stanford [ ] SHC/SCH [ ]  Other (specify): ­­­­
4. **Source(s) of Data** (select all that apply):

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

[ ] Registrar [ ] HR records [ ] Participant provided (e.g. surveys) [ ] Government data [ ] Other non-Stanford party

[ ] Other (describe):

**\***If you selected Epic or hospital medical records, explain in detail why you are using this system and whether the research can be conducted using STRIDE or another system.

1. **Processing Data.** Describe how and where the data will be collected, used, disclosed, stored and destroyed.
2. **Data will be:** [ ] Fully de-identified [ ] Identifiable

If “Fully de-identified,” describe the de-identification process, and explain who will be doing the de-identification.

1. **Data Elements**. 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)

[ ] Geographic subdivisions smaller than a state

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

[ ] Telephone numbers

 [ ] Fax numbers

 [ ] E-mail addresses

 [ ] Social Security numbers

 [ ] Medical record numbers

 [ ] Health plan beneficiary numbers

 [ ] Account numbers

 [ ] Certificate/license numbers

 [ ] Vehicle identifiers and serial numbers, including

 license plate numbers

 [ ] Device identifiers and serial numbers

 [ ] Web URLs

 [ ] IP address numbers

 [ ] Biometric identifiers, including finger and voiceprints

 [ ] Full face photographic images and any comparable

 images

 [ ] Any other unique identifying numbers, characteristic,

 or code (describe):

 [ ]  Other photographic images, video or audio

 [ ]  Stanford ID number (student, employee)

[ ] Lab or pathology test results

[ ] Diagnoses or procedures

[ ] Psychology or mental health information

[ ] Clinical records

[ ] Prescriptions or medications

[ ] Images or radiology reports

[ ] Other health, medical, physical, or mental status information (describe):

[ ]  Passport or Visa numbers

[ ] Employee personnel files

[ ]  Grades or performance (students, alumni)

[ ]  Disciplinary actions or proceedings (students, alumni)

[ ]  Demographics

[ ]  Financial account numbers

[ ] Financial records, including credit card or bank information

[ ] Donor contact and gift information

[ ] Salary information

[ ] Employment benefits

[ ] Other:

1. **INFORMATION ABOUT ADMINISTRATIVE SAFEGUARDS, APPLICATIONS, SYSTEMS, and DATA FLOW** *To complete this section, you may need to consult with the technical and security staff who administer the systems involved.**If a Third Party is involved, they should complete this section.*
2. **Name and Contact information for Third Party’s Privacy Officer and Security Officer.**
3. **Audits, Certifications, and Attestations.**

The non-Stanford party has attached the following annual third party audit report, certification, or attestation covering its privacy, security and IT operations and processes, including its 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

[ ]  Soc 2, Type 2 [ ]  FEDRAMP [ ]  Other (describe)

[ ]  None (explain below)

1. **Application Authentication.**
2. Provide the application URL in support of this project, if applicable.
3. Does it support Security Assertion Markup Language (SAML)? [ ]  Yes [ ]  No

**If no,**

1. Does it support two-step authentication? [ ]  Yes [ ] No
2. What are the password rules/syntax supported?
3. **Hosting Environment.** Identify environment (e.g. Amazon Web Services, physical data center, etc.).
4. **Data Flow.**
5. **Diagram and System Components.** Attach a diagram(s) depicting the proposed data flow in detail. Diagram should include details, such as protocols, ports, IP addresses, and physical location of each system component.
6. **Storage, Retention, and Destruction.** Provide a data flow description for each stage of the data lifecycle (collection, storage, use, transmission, access, and destruction). Describe where the data will be stored, and any physical, technical and administrative safeguards in place.
7. **Interface/Transmission.** 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.
8. **Data in Transit.**
9. What protocols are supported and enabled to transmit application-encrypted data? Select all that apply.

[ ] SSL v3 [ ] TLS 1.0 [ ] TLS 1.1 [ ] TLS 1.2 [ ] Other (specify)

1. Describe how data is transmitted from other systems. [ ]  Push [ ] Pull
2. **Data at Rest**
3. Is data encrypted at rest? [ ]  Yes [ ]  No
4. Are backups encrypted? [ ]  Yes [ ]  No
5. Describe how encryption keys are being secured, including who has access to the keys.
6. **Access.**
7. **Users and Administrators.** Identify the individuals or classes of individuals who will have administrator access and who will have user access to the system. Explain who manages access.
8. **Methods.** Identify the methods of user access to the system.