# University of California San Diego

**Request for Privacy Risk Assessment**

**Use this form to request a privacy risk assessment of programs or projects that involve moderate or high risk personal information. These are defined as P-3 and P-4 information, respectively, under the University of California** [**BFS-IS-3**](https://policy.ucop.edu/doc/7000543/BFB-IS-3) **policy.**

As you complete the form, please note the following:

Please download and complete this form. Do not complete this form on your browser. Download the file to your device before starting.



Sections A and B must be completed **by the UC San Diego requester**; Section C must be completed by third parties/vendors involved in the project (if any).



Attach all required documents. If required documents are not attached, reviews may be delayed.

Email the completed form and **all required attachments** to the Campus Privacy Office at ucsdprivacy@ucsd.edu, cc pparsi@ucsd.edu, for review. **Incomplete forms may be returned without review**.

Thank you!

**Privacy Risk Assessment**

Reviewer Use Only Request #-

Intake Form

|  |
| --- |
| **UC SAN DIEGO APPLICANT** |
| REQUESTOR NAME AND TITLE |
| **IF NOT SAME AS ABOVE,** PROJECT LEAD NAME AND TITLE |
| REQUESTING DEPARTMENT/UNIT |
| 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) |

1. **TO BE COMPLETED BY UCSD DEPARTMENT: INFORMATION ABOUT THE PROJECT**

Please review the data classification levels (*i.e.*, P-levels) in [BFS-IS-3](https://policy.ucop.edu/doc/7000543/BFB-IS-3) before completing this form; data should be classified at the highest level of sensitivity applicable. If unsure of the risk level, err on the side of the higher P-level.

1. **Overview.**
2. Identify all **non-UC San Diego** parties involved in the project. Add additional lines as necessary.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Entity name** | **Role** (e.g., vendor, funding sponsor, business associate, subcontractor, collaborator, technical support, etc.) | **Point of Contact** | **P-3 Data will be transferred to/accessed/collected by entity** | **P-4 Data will be transferred to/accessed/collected by entity** |
|  |  |  | Yes No | Yes No |
|  |  |  | Yes No | Yes No |

A signed [Appendix DS](https://www.ucop.edu/procurement-services/policies-forms/legal-forms-current/appendix-data-security.pdf) will be required, at minimum, from the third party for projects involving P-3 and P-4 data. The Campus Privacy Office strongly suggests that this document be provided to all vendors in advance for their review.

1. In layperson’s language, briefly summarize the overall project and purpose, including the contributions of all parties identified above. Explain what need you are trying to address.
2. What is the target start date for this project or this project phase? What is the expected period of performance?
3. Is this a new project or an enhancement/adjustment to an existing project?

[ ] New [ ] Enhancement/Adjustment

If this is an enhancement/adjustment, what is being changed?

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

1. **Project Funding.**  If this project is externally funded, provide the name of the funding source, record number, or agreement.

Name of Funding Source:

Is the funding under federal grant or contract? Agreement #:

[ ]  Project is not externally funded

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

[ ]  No known obligations [ ]  UC Terms and Conditions with Appendix DS

[ ]  MOUs [ ]  UC Terms and Conditions WITHOUT Appendix DS

[ ]  Master Agreement [ ]  Non-disclosure/Confidentiality Agreement [ ]  Umbrella Agreement [ ]  Sponsored Research Agreement [ ]  Business Associate Agreement (BAA) [ ]  Data Use Agreement

[ ]  Collaborative Agreement [ ]  FIPS, FISMA, NIST requirements in contract

[ ]  Statements of Work [ ]  Service Level Agreements (SLAs)

[ ]  Other (explain):

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

[ ]  Campus Counsel [ ]  Integrated Procure-to-Pay Solutions (IPPS) [ ]  Office of Contracts and Grants Administration [ ]  Export Control

[ ]  Office of Innovation and Commercialization [ ]  Advancement [ ]  Office of Risk Management

[ ]  Registrar [ ]  Health Sciences Compliance and Privacy

[ ]  Institutional Review Board (IRB) [ ]  UCOP [ ]  Information Technology Services (ITS)

[ ]  Other University schools or units:

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

1. **Access.** Who at UC San Diego will have access to the data and systems involved in this project? (Specific names, roles, or offices)
2. **Training.** Describe data management, privacy, and security trainings required for access. All UCSD workforce members with access to personal data must complete on-demand Privacy @ UCSD training through UC Learning.
3. **TO BE COMPLETED BY UCSD DEPARTMENT: INFORMATION ABOUT THE DATA INVOLVED IN PROJECT**
4. **Data Steward entity is:** [ ] Campus [ ] UCSD Health [ ]  Other (specify):
5. [**Data Steward**](https://blink.ucsd.edu/technology/bi/governance/council.html) **is:**
6. **Are the data incoming to/outgoing from the United States?** [ ] No [ ] Yes (where?):
7. **Data are accessed/Sourced from** (select all that apply):

[ ] ISIS [ ]  Activity Hubs [ ] Epic or hospital medical records**\*** [ ] Oracle Financials

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

[ ]  Clinical Data Warehouse for Research (CDWR) [ ] Other non-University system, database, or party

[ ] Other (describe):

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

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

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

1. **Population Location.** Some countries have very stringent privacy laws. If the data subject population is not entirely within the United States, specify the countries/regions in which data subjects are located physically.

 [ ]  US only [ ]  EU/UK [ ]  China [ ]  Canada [ ]  Brazil [ ]  India [ ]  Other (specify)

1. **Data Elements involved in any part of the project**. Select all that apply and explain, where necessary. Attach a data dictionary, if available. NOTE: Most apps and websites collect IP addresses and date-time stamps.

[ ] Full preferred names (students, alumni)

[ ] Full preferred names (patients, research subjects)

[ ] Full preferred names (employees)

[ ] Full preferred names (all others)

[ ] Legal names (any)

[ ] Partial names (*e.g.*, initials)

[ ] 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 addresses or MAC addresses

[ ] Biometric identifiers, including finger and voice prints

[ ] Full face photographic images and any comparable images

[ ]  Other photographic images, video or audio

[ ]  University ID number (student, employee)

[ ] Lab or pathology test results

[ ] Diagnoses or procedures

[ ] Psychology or mental health information

[ ] Drug use information

[ ] Clinical records

[ ] Prescriptions or medications

[ ] Images or radiology reports

[ ] Genetic information/test results

[ ]  Passport or Visa numbers

[ ] Employee personnel files

[ ]  Grades or performance (students, alumni)

[ ]  Disciplinary actions or proceedings (students, alumni)

[ ]  Race/ethnicity

[ ]  Sexual orientation or gender identity

[ ]  Veteran status

[ ]  Financial need/Pell Grant status

[ ]  Disability status

[ ]  Financial account numbers

[ ] Financial records, including credit card or bank information

[ ] Background checks/information

[ ] Information about crimes or criminal activity

[ ] Donor contact and gift information

[ ] Salary information

[ ] Employment benefits/beneficiaries

[ ] Athletic performance information

[ ] Political, religious, or philosophical beliefs

[ ] Comments, posts, survey responses, free text

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

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

[ ] Other:

1. **Explain the need for each type of data involved. Describe efforts to ensure that only the minimum necessary data are used/processed.**
2. **Will data be subject to any disclosure limitation methods (*e.g.*, de-identification, anonymization, differential privacy, or other masking) at any point in the data lifecycle (by UCSD or any vendors/third parties)?**

[ ] Yes [ ]  No

If you choose “Yes” above, describe the process, and explain who will be responsible for it (third party or UCSD).

1. **How will individuals whose data are involved be made aware of this data use and UC San Diego’s data practices?**

[ ] Consent (attach document or language) [ ] Website notice/Statement (attach)

 [ ] Opt-in [ ] Opt-out

[ ] Hard copy notice/statement

[ ] They will not be aware (explain)

* 1. Are there alternative ways for individuals to participate in this project without use of this platform/service? In other words, if someone opts out of this data use, are there alternatives for them? [ ] Yes [ ]  No
	2. Please describe what happens if an individual objects to use of this platform/service (*e.g.*, they will be unable to participate; they can participate with their camera off; this project is completely voluntary).
1. **Will other UC San Diego units have access to this information (*e.g.*, through activity hubs, shared for administration or analytics)?**

[ ] Yes [ ]  No

If yes, please describe who will have access and for what purpose.

1. **Will this information be combined with data from other sources?**

[ ] Yes [ ]  No

If yes, please describe what data will be combined and for what purpose.

1. **Please describe how you and any other group or entity handling the data will address any requests from the data subjects (*e.g.*, access, deletion, or correction requests) and who will be responsible for responding.**
2. **How long will the data be retained by UC San Diego?**
3. **What is the disposition of the data at the end of this project?**

[ ]  Securely deleted [ ]  Masked and archived (explain where)

[ ]  Masked and made available for open/public access (where)

1. **Does any part of this project involve a web/app tracking component (*e.g.*, use of web tracking pixels, cookies)?**

 [ ] Yes [ ]  No

If yes, describe tool, data collected by the tool, and the justification and need for tracking users.

**C. FOR VENDOR OR TECHNICAL/SECURITY STAFF TO COMPLETE: INFORMATION ABOUT ADMINISTRATIVE SAFEGUARDS, APPLICATIONS, SYSTEMS, and DATA USE AND FLOW OUTSIDE UNIVERSITY**

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

Name**:**

Contact:

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

Name**:**

Contact:

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. Note that out-of-date SOC reports will not be sufficient.

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

[ ]  Soc 2, Type 2 [ ]  FEDRAMP [ ]  None (**If None**, please move to question 4)

[ ]  Other (describe below)

1. **Self-Disclosures and other documentation.**

Please specify **and attach** the most recent self-disclosures or attestations covering privacy, security and IT operations and processes, including risk assessment and risk management process; data collection, use, disclosure, storage and destruction policies; data subject rights and complaint handling; 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.

[ ]  HECVAT [ ]  EU-US Privacy Shield [ ]  Swiss-US Privacy Shield

[ ]  None (**If None**, please attach internal Privacy Policies and Information Security Policies)

[ ]  Other (describe below)

1. **Application Authentication.**
2. Does your application support two-step authentication? [ ]  Yes [ ]  No

If so, please specify:

1. Provide the application URL in support of this project, if applicable.
2. 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 complexity requirements (e.g., minimum 8 characters, alphanumeric, etc)?
3. **Hosting Environment.** Identify the hosting environment (*e.g.*, Amazon Web Services, physical data center, etc.), backup environment and geographical location of each.
4. **Data Use.** Do you use any data, including “de-identified” or “anonymized” data, collected for, from, or on behalf of the University for any other purpose than providing the services for the project above (*e.g.*, your own analytics, training algorithms, facial recognition, marketing, creating profiles of individuals or institutions)?

 [ ] Yes [ ]  No

* 1. Do you create a profile of users? [ ] Yes [ ]  No
	2. Do you combine data from this project with data from other sources? [ ] Yes [ ]  No

If you answered “Yes” to any of the above, please explain.

1. **Data Sharing.** Do you share, disclose, or sell any data, including “de-identified” or “anonymized” data, collected for, from, or on behalf of the University to any other entity, including your affiliated entities, subsidiaries, parent organizations, or government entities?

 [ ] Yes [ ]  No

If yes, please describe to whom you disclose information.

1. **Other Data Processing and Code Reviews.**
2. Do you “de-identify” or “anonymize” data collected for, from, or on behalf of the university for any use other than the project? [ ] Yes [ ]  No

If you answered “Yes” to any of the above, please explain by what standard you de-identify information and what processes you use.

1. Do you have a documented policy for reviewing codes, processes, and algorithms for bias and discrimination? If so, please attach. [ ] Yes [ ]  No
2. **Data Flow.**
3. **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 [P3 or P4](https://security.ucop.edu/policies/institutional-information-and-it-resource-classification.html) information with another system.
4. **Storage, Retention and Destruction.** Provide a data flow description for each stage of the data lifecycle (collection, storage, use, transmission, access, and destruction).
5. **Data in Transit.**
6. What protocols are supported and enabled to transmit application encrypted data? Select all that apply.

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

1. Is University initiating the transaction? [ ]  Yes [ ] No
2. Is University pushing or pulling data from other vendor systems? [ ] Pushing [ ] Pulling [ ] Both
3. **Data at Rest.**
4. Are data encrypted at rest? [ ]  Yes [ ]  No
5. Are backups encrypted? [ ]  Yes [ ]  No
6. Describe where encryption keys are stored and how they are being secured, including who has access to the keys.
7. **Access.**
8. **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.
9. **User Methods.** Check the different methods by which the users can access the system

 [ ] SSH [ ] Web Application [ ] Client Application [ ] Other (specify)

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

 [ ] SSH [ ] Web Application [ ] Client Application [ ] Other (specify)

1. **Insurance.**
2. Do you have cyberinsurance covering the proposed services? [ ]  Yes [ ]  No
3. Provide details of your cyberinsurance protection, including amount of coverage and what is covered.