**Part 1: Data Recipient Questionnaire**

1. Reference number for dataset Data Recipient wishes to access:
2. Title of the project Data Recipient intends to undertake with the Data:
3. Data Recipient name:
4. Address:
5. Phone number:
6. Email:
7. Data Recipient’s largest shareholder or partner (if a corporation or partnership):
8. Has Data Recipient previously executed a data agreement with the University of California? Yes  No
9. Has Data Recipient ever experienced an event where sensitive health data in the custody of Data Recipient was inadvertently acquired, accessed, used, or disclosed to a third party (data breach)? Yes  No

*If yes, provide details of each event here.*

1. What is the project outcome or endpoint Data Recipient is intending to achieve with the Data?
2. Can the Data Recipient achieve this project outcome without accessing this Data from UCSF?
3. How does this project outcome improve the health of the people of California and globally?
4. Will Data Recipient ensure Data never leaves the United States? Yes  No
5. Does Data Recipient have a Security Plan that can be audited upon request? Yes  No
6. Does Data Recipient have a research plan which depicts the project the Data will be used in? Yes  No

**Part 2: Agreement**

This Data Sharing Agreement (“Agreement”) is made by and between The Regents of the University of California, a California public corporation, on behalf of its University of California San Francisco campus (“UC” or “UCSF”), and the Data Recipient named below in the signature block (“Data Recipient”). UCSF and Data Recipient are each referred to in this Agreement as a “Party” and together, the “Parties.”

Whereas, Data Recipient desires to receive Data for the Project, both of which are defined below, and agrees to comply with the terms and conditions of this Agreement; and

Whereas, UCSF anticipates that Data Recipient’s receipt and use of Data for this purpose will result in a tangible outcome that directly or indirectly benefits UCSF’s mission, patients and society, and thus desires to provide Data to Data Recipient under the terms and conditions of this Agreement.

Now, therefore, in consideration of the mutual promises contained herein and for other good and valuable consideration that each Party acknowledges is sufficient, the Parties agree as follows:

1. **Definitions**
2. “Data” includes all information set forth in Exhibit 1, which is provided by UCSF to Data Recipient or to which UCSF provides access to Data Recipient. “Data” also includes any derivation of information set forth in Exhibit 1, irrespective of how trivial or complex the derivation may be, including but not limited to de-identified Data.
3. “Data Breach” means the acquisition, access, use, or disclosure of Data in a manner not permitted under this Agreement.
4. “Major Change” means the implementation of a change that could affect the security of Data or UCSF Information Resources, including changes to architectures, processes, tools, metrics, and documentation, and configuration.
5. “Project” means the activity described in Exhibit 1, for which UCSF is providing Data to Data Recipient.
6. “Research Data Archive” means: a catalogue of datasets available for licensing on the Innovation Ventures website.
7. “Security Incident” means: (1) a material compromise of the confidentiality, integrity, or availability of Data or UCSF Information Resources; (2) a single event or a series of unwanted or unexpected events that has a significant probability of compromising UCSF business operations or threatening Data or UCSF Information Resources; (3) any event involving a cyberintrusion that potentially affects Data or UCSF Information Resources; or (4) a material failure of Data Recipient’s administrative, technical, or physical controls that resulted or could have resulted in an adverse impact to the confidentiality, integrity, or availability of Data or UCSF Information Resources.
8. “UCSF Confidential Information” means any Data that is (i) marked as “Confidential” at the time of disclosure; (ii) if disclosed orally, identified at the time of such oral disclosure as confidential, and reduced to writing as “Confidential” within thirty (30) days of such oral disclosure; or (iii) if not marked as “Confidential,” information that would be considered by a reasonable person in the relevant field to be confidential given its content and the circumstances of its disclosure. Information will not be considered UCSF Confidential Information to the extent that: (i) Data Recipient can demonstrate by written records that it was known to Data Recipient before the effective date of the Agreement; (ii) it is currently in, or in the future enters, the public domain other than through a breach of the Agreement or through other acts or omissions of Data Recipient; (iii) it is obtained lawfully from a third party; or (iv) it is disclosed under the California Public Records Act or legal process.
9. “UCSF Information Resources” means IT infrastructure, cloud services, software, and/or hardware with computing and/or networking capability owned or managed by UCSF, or a Data Recipient-owned infrastructure, cloud services, software, and/or hardware that is connected to UCSF systems or networks or that is used for UCSF business.
10. **UCSF Provision of Data**
11. Provision of Data. UCSF will provide Data to Data Recipient for the Project, as set forth in Exhibit 1. UCSF may withhold Data that UCSF determines, in its sole discretion, it may not provide to Data Recipient under federal, state, or international laws, UCSF or UC policies, or its existing contractual obligations to third parties.
12. Ownership of Data. UCSF retains all title to and rights in Data. UCSF hereby grants to Data Recipient a non-exclusive, non-sublicensable license to Data for the sole purpose of conducting the Project.
13. No Exclusivity. Data Recipient agrees that this Agreement will not prohibit or otherwise limit the use or disclosure by UCSF or other campuses of the University of California (collectively, “UC”) for any research, patient care, educational purpose, or other purpose for any time period.
14. Intellectual Property Rights. This Agreement does not confer on Data Recipient any patent, copyright, trademark, license right or trade secret (“Intellectual Property Rights”) owned or obtained by UC. Any agreement related to Intellectual Property Rights will be handled by a separate agreement between the Parties.
15. **Cost Recovery**

For cost recovery purposes, Data Recipient will pay UCSF a non-refundable annual subscription fee of $22,500 per dataset upon UCSF countersigning this Agreement (Effective Date) and upon each anniversary of this Agreements Effective Date (Renewal Date). This annual subscription fee covers the estimated direct and indirect costs incurred by UCSF to prepare the Data and maintain the Research Data Archive. Data Recipient will continue to pay the annual subscription fee upon each Renewal Date, so long as:

1. the tools, programs, algorithms, products, or services created, trained, or validated with the Data were used (internally or externally to Data Recipient) at least once in the 6-month period preceding the Renewal Date.

OR

1. Data Recipient has not destroyed the dataset per section 12.C.1, by the Renewal Date.

This section (3) survives termination of this Agreement.

1. **Purpose and Use Restrictions on Data**
2. Use of Data for Project Only; No Other Access, Use or Disclosure of Data. Subject to Section 8 (Publication), Data Recipient may access, use and disclose Data only for purposes of the Project; any other use will constitute a material breach of this Agreement. Data Recipient may allow its employees to access Data provided that: (i) Data Recipient discloses only such Data as is necessary for the Data Recipient to perform the Project, and (ii) Data Recipient informs such employees of the obligations of confidentiality governing the access, use and disclosure of Data before Data Recipient disclosure. Data Recipient may not sell, lease or transfer other rights to Data, may not transfer, disclose or make available Data to any third party, affiliate, contractor, vendor, or partner, and may not assign its obligations or rights under this Agreement without an express written amendment to this Agreement. Data Recipient may not permit access to any Data by an application or an application developer (whether developed or controlled by Data Recipient, a Data Recipient affiliate, or a third party) without express advance written permission by UCSF and acceptance of all relevant requirements of this Agreement by such application developer. Data Recipient may not access or use Data to build or contribute to a consumer or other profile database.
3. Prohibition on Re-identification of Individuals. If Data Recipient receives Data in a form that does not identify individuals, Data Recipient may not use any Data, either alone or in combination with other data that is currently or in the future in the possession of Data Recipient, to identify any individual in the Data, nor enable any third party to identify any individual in the Data, and Data Recipient may not knowingly attempt to contact any individual whose Data has been provided to Data Recipient. Data Recipient will notify UCSF immediately if Data Recipient identifies an individual, or if it becomes aware that a third party has done so.
4. Data Linkage. Data Recipient may not link, combine, hash, concatenate, aggregate or add together Data in any way with any other data sources or information without the express written approval of UCSF.
5. Data to Stay Within the United States; No Offshoring. Data Recipient's transmission, export, transportation, or storage of Data out of the United States, or access to Data from outside the United States, is prohibited.
6. Compliance with Applicable Laws. Data Recipient agrees to comply with all state, federal and international laws that are applicable to UCSF and to Data Recipient, any instructions provided by UCSF, as well as industry best practices that govern the collection, access, use, disclosure, safeguarding and destruction of Data.
7. Future Restrictions. In the event UCSF or any state or federal agency promulgate guidance or policy or enacts laws or rules regarding the exchange of data that conflict with the terms of this Agreement, the Parties agree to negotiate in good faith to amend the Agreement to account for such additions or changes in guidance, policy, law or rule. Should the Parties not agree on amended terms to the Agreement within sixty (60) days of UCSF's notice to Data Recipient of the required renegotiation, UCSF may immediately terminate the Agreement.
8. Notice of External Request or Legal Requirement to Disclose. If required by a court of competent jurisdiction or an administrative body to disclose Data, Data Recipient will notify UCSF in writing immediately upon receiving notice of such requirement and before any such disclosure, to give UCSF an opportunity to oppose or otherwise respond to such disclosure (unless prohibited by law from doing so). To the extent Data Recipient still is required to disclose Data, Data Recipient will furnish only that portion that is legally required and will exercise all reasonable efforts to obtain reliable assurance that confidential treatment will be afforded to any Data disclosed.
9. Notice of Complaint, Litigation or Investigation. Data Recipient will notify UCSF immediately, both orally and in writing, but in no event more than two (2) business days after Data Recipient receives a complaint from an individual about the use of Data, the filing of a claim or threatened filing of a claim, or correspondence indicating a regulatory agency is or will be conducting an investigation.
10. Treatment of Data in Litigation. In the event litigation is brought against UCSF by any individual seeking a return or destruction of Data, and UCSF notifies Data Recipient of such litigation, Data Recipient will: (i) destroy any Data if ordered by a court to do so, or (ii) handle Data in an alternative manner consistent with law, as agreed upon by Data Recipient and the parties to such litigation. UCSF may not agree with any third party to destroy Data in Data Recipient's possession absent consultation with Data Recipient and negotiation in good faith with Data Recipient's participation.
11. Conflict in Terms. If applicable, Appendix-BAA and/or Appendix-GDPR will control in the event and to the extent one or more appendices is incorporated into the Agreement and conflicts with the provisions of this Section 4.
12. **Data Security**

Data Recipient must provide commercially acceptable cybersecurity and risk management to protect Data and UCSF Information Resources. Such measures include, but are not limited to the following:

1. Compliance with UCSF Instructions. Data Recipient must follow all instructions UCSF provides in writing to Data Recipient.
2. Risk Assessment. Data Recipient must conduct an accurate and thorough assessment of the potential risks to, and vulnerabilities of, the security of the Data and UCSF Information Resources. Data Recipient must mitigate anticipated risks effectively, including implementing commercially acceptable security policies, procedures, and practices that protect Data and UCSF Information Resources. Data Recipient must keep UCSF informed with timely updates on risks, vulnerabilities, and security incidents, including any measures UCSF must undertake to ensure the security of Data and UCSF Information Resources.
3. Compliance with Data Security Plan. Data Recipient must develop and document a plan that protects Data and UCSF Information Resources, which conforms to a recognized cybersecurity framework designed for that purpose (the “Security Plan”). Data Recipient must responsibly execute the Security Plan. Data Recipient must provide its Security Plan to UCSF upon request by UCSF. The Security Plan must:
4. Ensure the security (including but not limited to: confidentiality, integrity, and availability) of Data and UCSF Information Resources through the use and maintenance of appropriate administrative, technical, and physical controls;
5. Protect against any reasonably anticipated threats or hazards to Data and UCSF Information Resources;
6. Address the risks associated with Data Recipient having access to Data and UCSF Information Resources;
7. Comply with all applicable legal and regulatory requirements for data protection, security, and privacy;
8. Clearly document Data Recipient’s cybersecurity responsibilities;
9. Prevent the sharing of passwords or authentication secrets that provide access to Data and UCSF Information Resources;
10. Prevent the use of shared passphrases (passwords) or other authentication secrets;
11. Prevent unauthorized access to Data and UCSF Information Resources;
12. Prevent unauthorized changes to UCSF Information Resources;
13. Prevent the reduction, removal, or turning off of any security control without express written approval from UC;
14. Prevent the storing, harvesting, or passing through of credentials (username, password, authentication secret, or other factor); and
15. Prevent the use or copying of Data and UCSF Information Resources for any purpose not authorized under the Agreement.
16. Update to Data Security Plan. Data Recipient must update its Security Plan to effectively address new cybersecurity risks, at least annually and within fifteen (15) days into the next calendar quarter following a Major Change. Data Recipient must provide its updated Security Plan to UCSF upon request by UCSF.
17. Requests from UCSF and Evidence of Compliance.
18. Upon request by UCSF, Data Recipient must provide UCSF with evidence that demonstrates to UCSF’s reasonable satisfaction Data Recipient’s adherence to its Security Plan (including but not limited to providing a third-party report, attestation signed by an authorized individual, attestation of compliance by a qualified assessor, or a mutually agreed upon equivalent), upon reasonable request (including but not limited to (a) annually, (b) after Major Changes, and (c) as a result of a Security Incident), or as required by any applicable regulatory or governmental authority.
19. Data Recipient must respond to UCSF’s reasonable questions related to cybersecurity controls, Security Incidents, or Major Changes, newly published vulnerabilities, and/or risk assessments within ten (10) business days.
20. UCSF may request and perform a security audit using a qualified third party or a mutually agreed upon alternative annually or as a result of a Data Breach.
21. Notifications Required.
22. Data Recipient must notify UCSF of any Major Changes within twenty (20) business days of the Major Change. However, if Data Recipient makes any material modifications to its Security Plan that will adversely affect the security of Data or UCSF Information Resources, Data Recipient must notify UCSF within seventy-two (72) hours and identify the changes.
23. Data Recipient must notify UCSF of a Security Incident or Data Breach in accordance with Section 6 of this Agreement.
24. **Data Breaches and Security Incidents**

a. Reporting of Breach or Security Incident. If Data Recipient reasonably suspects that a Data Breach and/or a Security Incident has occurred that affects Data or UCSF Information Resources, Data Recipient must promptly notify UC both orally and in writing, using the contacts in the Agreement. Notification must occur within seventy-two (72) hours after discovery of the suspected Security Incident and/or Data Breach. Data Recipient’s notification must identify:

(1) Contacts for both technical and management coordination;

(2) Escalation and identifying information, such as ticket numbers, system identifiers, etc.;

(3) The nature of the Data Breach and/or Security Incident;

(4) The Data or UCSF Information Resources affected;

(5) What Data Recipient has done or will do to mitigate any deleterious effect; and

(6) What corrective action Data Recipient has taken or will take to prevent future Security Incidents or Data Breaches.

b. Information to Be Provided. Data Recipient will provide all information as reasonably requested by UCSF.

c. Progress Reports. In the event of a suspected Data Breach and/or Security Incident, Data Recipient will keep UCSF informed regularly of the progress of its investigation until the incident is resolved.

d. Coordination of Data Breach Response or Security Incident Activities. Data Recipient will fully cooperate with UCSF’s investigation of any Data Breach and/or Security Incident involving Data or UCSF Information Resources. Data Recipient’s full cooperation will include, but not be limited to, Data Recipient:

(1) Promptly preserving any potential forensic evidence relating to the Data Breach and/or Security Incident;

(2) Remedying the Data Breach and/or Security Incident as quickly as circumstances permit;

(3) Promptly, but no more than seventy-two (72) hours after the discovery of Data Breach and/or Security Incident, designating a contact person to whom UCSF will direct inquiries and who will communicate Data Recipient responses to UCSF inquiries;

(4) As rapidly as circumstances permit, assigning/using appropriate resources to remedy, investigate, and document the Data Breach and/or Security Incident and undertake appropriate response activities;

(5) Providing status reports to UCSF regarding Data Breach and Security Incident response activities, either on a daily basis or a frequency approved by UCSF;

(6) Coordinating all media, law enforcement, or other Data Breach and/or Security Incident notifications with UCSF in advance of such notification(s), unless expressly prohibited by law;

(7) Ensuring that knowledgeable Data Recipient employees are available on short notice, if needed, to participate in UCSF and Data Recipient initiated meetings and/or conference calls regarding the Data Breach and/or Security Incident; and

(8) Ensuring that knowledgeable Data Recipient employees and agents participate in after-action analysis, including root cause analysis and preventive action planning.

e. Corrective and Preventive Action. As a result of a Data Breach and/or Security Incident impacting Data and/or UCSF Information Resources, and upon UCSF’s request, Data Recipient must prepare a report detailing corrective and preventive actions. The report must include:

(1) A mutually agreed upon timeline for the corrective and preventive actions based on the nature of the Data Breach and/or Security Incident;

(2) Identification and description of the root causes; and

(3) Precise steps Data Recipient will take to address the failures in the underlying administrative, technical, and/or physical controls to mitigate damages and future cyber risk.

f. Costs. Data Recipient will reimburse UCSF for reasonable costs related to responding to Data Breaches or Security Incidents that affect Data or USCF Information Resources that are caused by Data Recipient. This includes all costs associated with notice and/or remediation of a Data Breach.

1. Grounds for Termination. Any Data Breach may be grounds for termination of the Agreement by UCSF. Agreement obligations to secure, dispose, and report continue through the resolution of the Data Breach and/or Security Incident.
2. **Use of UC Name and Trademarks**

Data Recipient will not use the UC name, abbreviation of the UC name, trade names and/or trademarks (i.e., logos and seals) or any derivation thereof, in any form or manner in advertisements, reports, or other information released to the public, or place the UC name, abbreviations, trade names and/or trademarks or any derivation thereof on any consumer goods, products, or services for sale or distribution to the public, without UC’s prior written approval. Data Recipient agrees to comply at all times with California Education Code Section 92000.

1. **Publication**

Any publication or presentation derived from the use of the Data must contribute in a meaningful way to improving the health of UCSF patients or society, and must include attribution to UCSF authors, as applicable, consistent with the guidelines of the International Committee of Medical Journal Editors. Data Recipient will furnish to UCSF a copy of any proposed publication or release at least forty-five (45) days in advance of the proposed submission or presentation date. Within this forty-five (45) day period, UCSF will review such proposed publication or release to determine whether it contains any Data, to determine whether UCSF desires to file patent applications on subject matter contained in the publication, or to ensure the accuracy of the information contained in the publication or release. Upon receiving any notification from UCSF requesting deletion of Data, correction of inaccuracies, or a delay in publication to allow the filing of patent applications before publication or release, Data Recipient will cooperate in taking the requested action.

**9. Insurance**

* 1. Required Coverage. Data Recipient, at its sole cost and expense, will obtain, keep in force, and maintain the following insurance with the minimum limits set forth below:
     1. Commercial Form General Liability Insurance (contractual liability included) with minimum limits as follows:
        + 1. Each Occurrence $1,000,000;
          2. General Aggregate $2,000,000.
     2. If applicable, Professional Liability Insurance with a limit of two million dollars ($1,000,000) per occurrence or claim with an aggregate of not less than two million dollars ($2,000,000). If this insurance is written on a claims-made form, it will continue for three years following termination of the Agreement. The insurance will have a retroactive date of placement prior to or coinciding with the effective date of the Agreement.
     3. Workers' Compensation as required by applicable state law and Employer’s Liability with limits of one million dollars ($1,000,000) per occurrence. Workers' Compensation as required by applicable state law and Employer’s Liability with limits of one million dollars ($1,000,000) per occurrence.
     4. Cyber Insurance, typically referred to as Privacy, Technology and Data Security Liability, Cyber Liability, or Technology Professional Liability insurance, which will cover liabilities for financial loss due to the acts, omissions, or intentional misconduct of Data Recipient and any Data Recipient Agent, in connection with the performance of this Agreement, as well as all Data Recipient costs, including damages it is obligated to pay UC or any third party, that are associated with any confirmed or suspected Data Breach or compromise of UCSF Information Resources. Regardless of the type of policy(ies) in place, such coverage will include without limitation: (i) costs to notify parties whose Data was lost or compromised; (ii) costs to provide credit monitoring and credit restoration services to parties whose Data was lost or compromised; (iii) costs associated with third party claims arising from the confirmed or suspected Data Breach or loss of Institutional Information, including litigation costs and settlement costs; (iv) any investigation, enforcement, fines and penalties, or similar miscellaneous costs; and (v) any payment made to a third party as a result of extortion related to a confirmed or suspected Data Breach. Such policy must have the following limits: **$5,000,000 each occurrence and $5,000,000 in the aggregate.**

**10. Indemnification and Limitation of Liability**

1. Data Recipient Indemnification. To the fullest extent permitted by law, Data Recipient will defend, indemnify, and hold harmless UC, its officers, employees, and agents, from and against all losses, expenses (including, without limitation, reasonable attorneys' fees and costs), damages, and liabilities of any kind resulting from or arising out of the Agreement, including the performance hereunder of Data Recipient, its officers, employees, agents, or anyone directly or indirectly employed by Data Recipient, or any person or persons under Data Recipient 's direction and control (collectively, “Data Recipient Agents”), provided such losses, expenses, damages and liabilities are due or claimed to be due to the acts or omissions of Data Recipient or a Data Recipient Agent.
2. Additional Indemnification Related to Data Breach or Compromise of UCSF Information Resources. Data Recipient’s indemnification obligations under this Agreement will include (without limitation) the following fees and costs that arise as a result of a Data Breach or a compromise of UCSF Information Resources caused by the negligent acts or omissions, or willful misconduct of Data Recipient or a Data Recipient Agent: any and all costs associated with notification to individuals or remedial measures offered to individuals, whether or not required by law, including but not limited to costs of notification of individuals, establishment and operation of call center(s), credit monitoring and/or identity restoration services; time of UCSF personnel responding to Data Breach; fees and costs incurred in litigation; the cost of external investigations; civil or criminal penalties levied against UCSF; civil judgments entered against UCSF; and attorneys’ fees, and court costs.
3. Attorneys’ Fees. In any action brought by a Party to enforce the terms of this Agreement, the prevailing Party will be entitled to reasonable attorney's fees and costs, including the reasonable value of any services provided by in-house counsel. The reasonable value of services provided by in-house counsel will be calculated by applying an hourly rate commensurate with prevailing market rates charged by attorneys in private practice for such services.
4. Notice. UCSF agrees to provide Data Recipient with prompt notice of any such claim or action and to permit Data Recipient to defend any claim or action, and that UCSF will cooperate fully in such defense. UCSF retains the right to participate in the defense against any such claim or action, and the right to consent to any settlement, which consent will not unreasonably be withheld.
5. LIMITATION OF LIABILITY. IN NO EVENT WILL UCSF BE LIABLE FOR ANY LOSS OF PROFITS; LOSS OF DATA; ANY INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES; OR ANY COSTS OF PROCUREMENT OF SUBSTITUTE DATA, EVEN IF UCSF HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH CLAIMS OR DEMANDS.
6. Assistance in Litigation or Administrative Proceedings. Data Recipient will make itself and any employees, subcontractors, or agents assisting Data Recipient in the performance of its obligations available to UCSF at no cost to UCSF to testify as witnesses, or otherwise, in the event of a Data Breach or other unauthorized disclosure of Data caused by Data Recipient that results in litigation, governmental investigations, or administrative proceedings against UCSF, its directors, officers, agents or employees based upon a claimed violation of laws relating to security and privacy or arising out of this Section.

**11. Warranties and Disclaimer of Warranties**

* 1. Data Recipient Warranties. Data Recipient acknowledges that failure to comply with any of the warranties in the Agreement will constitute a material breach of the Agreement and UCSF will have the right to terminate the Agreement without damage, penalty, cost or further obligation. Data Recipient represents, warrants and covenants that: (i) Data Recipient is free to enter into this Agreement; (ii) Data Recipient will comply with all applicable laws, rules and regulations in performing Data Recipient’s obligations hereunder; and (iii) Data Recipient is not presently debarred, suspended, proposed for debarment, or declared ineligible for award of federal contracts or participation in federal assistance programs or activities. The rights and remedies so provided are in addition to and do not limit any rights afforded to UCSF by any other article of the Agreement.
  2. UCSF Warranties. UCSF acknowledges that failure to comply with any of the warranties in the Agreement will constitute a material breach of the Agreement and Data Recipient will have the right to terminate the Agreement without damage, penalty, cost or further obligation. UCSF represents, warrants and covenants that UCSF is free to enter into this Agreement and that it has the right and authority to provide Data to Data Recipient. EXCEPT AS SET FORTH HEREIN, THE DATA ARE PROVIDED "AS IS," AND UCSF HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE. UCSF SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, UCSF MAKES NO WARRANTY OF ANY KIND THAT THE DATA WILL BE AVAILABLE AT ALL TIMES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE OR ERROR-FREE.

**12. Term of Agreement/Termination**

1. Term.

The term of the Agreement will be **5 years** from the Effective Dateand is subject to earlier termination as provided below. It may be extended upon the agreement of the Parties.

1. Termination.
2. Termination for Convenience. UCSF may terminate the Agreement for convenience by giving Data Recipient at least **30** calendar days' written notice.
3. Termination for Cause. UCSF or Data Recipient may terminate the Agreement for a material breach of the Agreement upon notice to the breaching Party.
4. Termination for Insolvency or Bankruptcy. UCSF may terminate this Agreement if Data Recipient: (i) becomes insolvent; makes a transfer in fraud of creditors; makes an assignment for the benefit of creditors; or admits, in writing, its inability to pay its debts as they become due; (ii) commits an act of bankruptcy; files a petition under the United States Bankruptcy Code or under any other similar federal or state law; is adjudged bankrupt; or is named in a pleading or motion filed in any court proposing to reorganize or adjudicate as a bankrupt, and that pleading or motion is not discharged or denied within sixty (60) days after its filing; (iii) has a receiver or trustee appointed for all or substantially all of its assets, and the receiver or trustee is not discharged within sixty (60) days after its appointment; (iv) has filed against it any tax lien respecting all or substantially all of its property and such tax lien shall not be discharged, removed, or bonded over within sixty (60) days of the date on which it was filed; or (v) has its assets assigned by law.
5. Disposition of Data at Termination.
6. Deletion or Destruction of Data. Within thirty (30) days of termination, cancelation, expiration or other conclusion of this Agreement, Data Recipient will permanently delete and destroy all Data. This provision will also apply to all Data that is in the possession of any agents or subcontractors of Data Recipient (to the extent that UCSF has agreed in writing that Data Recipient may provide Data to Data Recipient agents or subcontractors). Such deletion and/or destruction will be accomplished by "purging" and/or "physical destruction," in accordance with the National Institute of Standards and Technology Special Publication 800-88. Data Recipient will certify in writing to UCSF that such deletion has been completed. If Data Recipient reasonably believes that deletion of Data is technically impossible or impractical, Data Recipient must provide UCSF with an annual written statement of the reason that deletion or destruction is impossible or impractical. Transformation of the Data or concatenation of Data with other data from non-UCSF sources shall not constitute technical impossibility or impracticality for purposes of this Agreement. If UCSF determines, in its sole discretion, that deletion or destruction is technically impossible or impractical, Data Recipient shall continue to protect the Data in accordance with the terms of this Agreement.
7. Insolvency or Bankruptcy. In the case of termination by UCSF for bankruptcy or insolvency by the Data Recipient, Data Recipient shall, automatically and without any further actions of the Parties, assign all rights, title and interest in and to the Data to UCSF, and Data Recipient shall destroy any Data remaining in its possession.
8. Survival. Upon expiration or termination of the Agreement, or if Data will not be returned or deleted pursuant to Section 13(c)(1), the following provisions will survive: (i) Section 1, Definitions; (ii) Section 2b-d, Provision of Data; (iii) Section 3 (Cost Recovery); iv) Section 4 (Purpose and Use Restrictions on Data); (v) Section 5, Data Security; (vi) Section 6, Data Breaches and Security Incidents, (vii) Section 7, Use of UC Name and Trademarks, (viii) Section 10, Insurance, (ix) Section 11, Indemnification and Limitation of Liability, (x) Section 12, Warranties and Disclaimer of Warranties, (xi) Section 13c, Disposition of Data at Termination, (xii) Section 14, Miscellaneous, and (xiii) the terms of the APPENDIX–BAA BUSINESS ASSOCIATES, and/or APPENDIX-GDPR, as applicable.

**14**. **Miscellaneous**

* 1. Incorporated Documents. Incorporated Documents may include, as applicable:

(1) UC Appendix–Business Associate (HIPAA), at https://www.ucop.edu/procurement-services/\_files/Legal%20docs/appendix-ba.pdf

* 1. Entire Agreement. This Agreement and its Incorporated Documents contain the entire Agreement between the Parties and supersede all prior written or oral agreements with respect to the subject matter herein.
  2. Severability. If a provision of the Agreement becomes, or is determined to be, illegal, invalid, or unenforceable, that will not affect the legality, validity or enforceability of any other provision of the Agreement or of any portion of the invalidated provision that remains legal, valid, or enforceable.
  3. Waiver. Waiver or non-enforcement by either Party of a provision of the Agreement will not constitute a waiver or non-enforcement of any other provision or of any subsequent breach of the same or similar provision.
  4. Remedies. Data Recipient acknowledges that remedies at law would be inadequate to protect UCSF against any actual or threatened breach of this Agreement by Data Recipient, and, without prejudice to any other rights and remedies otherwise available to UCSF, Data Recipient agrees to the granting of injunctive relief in UCSF’s favor without proof of actual damages.
  5. Governing Law and Venue. California law will control the Agreement, its Exhibits and Appendices. The exclusive jurisdiction and venue for any and all actions arising out of or brought under the Agreement is in a state court of competent jurisdiction, situated in the county of San Francisco, California.
  6. Assistance in Litigation or Administrative Proceedings. Data Recipient will make itself and its employees, subcontractors, or agents assisting Data Recipient in the performance of its obligations available to UCSF at no cost to UCSF to testify as witnesses, or otherwise, in the event of investigations, or proceedings against UCSF, its directors, officers, agents, or employees relating to the Agreement.
  7. Independent Contractors. At no time will Data Recipient or Data Recipient’s employees, agents, or assigns be considered employees of UCSF for any purpose, including but not limited to workers’ compensation provisions. Data Recipient shall not have the power nor right to bind or obligate UCSF, and Data Recipient shall not hold itself out as having such authority. Data Recipient shall be responsible for its employees, agents and subcontractors, including being responsible for ensuring payment of all unemployment, social security, payroll, contributions and other taxes with respect to such employees, agents and subcontractors.
  8. Force Majeure. Neither Party will be liable for delays due to causes beyond the Party’s control (including, but not restricted to, war, civil disturbances, earthquakes, fires, floods, epidemics, quarantine restrictions, freight embargoes, and unusually severe weather).
  9. Assignment and Subcontracting. Except as to any payment due hereunder, Data Recipient may not assign or subcontract the Agreement without UCSF’s written consent. In case such consent is given, the assignee or subcontractor will be subject to all of the terms of the Agreement.
  10. No Third-Party Rights. Nothing in the Agreement, express or implied, is intended to make any person or entity that is not a signer to the Agreement a third-party beneficiary of any right created by this Agreement or by operation of law.
  11. Other Applicable Laws. Any provision required to be included in a contract of this type by any applicable and valid federal, state or local law, ordinance, rule or regulations will be deemed to be incorporated herein.
  12. Auditing. Data Recipient shall make available to UCSF all products, systems, and documents as necessary to allow UCSF to audit Data Recipient's compliance with this Agreement.
  13. Notices. A Party must send any notice required to be given under the Agreement by overnight delivery or by certified mail with return receipt requested, to the other Party’s representative at the address specified below the signature blocks below, or as updated in writing by a Party from time to time.
  14. Authorized Signatory. This Agreement is binding only if it is negotiated and executed by an authorized representative with the proper delegation of authority.

**THE REGENTS OF THE [DATA RECIPIENT NAME]**

**UNIVERSITY OF CALIFORNIA**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Signature) (Signature)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Printed Name, Title) (Printed Name, Title)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Date) (Date)

NOTE: Please send (1) completed questionnaire (2) signed agreement (3) completed Appendix A and (4) supporting research plan documentation to [innovation@ucsf.edu](mailto:innovation@ucsf.edu)

**Notice:**

To UCSF regarding confirmed or suspected Data Breach:

|  |  |
| --- | --- |
| **Name** |  |
| **Phone** |  |
| **Email** |  |
| **Address** |  |
|  |  |

To UCSF regarding contract issues not addressed above:

|  |  |
| --- | --- |
| **Name** |  |
| **Phone** |  |
| **Email** |  |
| **Address** |  |
|  |  |

To Data Recipient:

|  |  |
| --- | --- |
| **Name** |  |
| **Phone** |  |
| **Email** |  |
| **Address** |  |
|  |  |

**Exhibit 1: Project and Data**

1. Data Recipient’s Project Title:

2. Data:

* 1. Reference Number:
  2. Field:
  3. Scope:
  4. Lead Investigator: