|  |  |  |
| --- | --- | --- |
| **dhcs_logo_color_v1_1a** | **State of California****Department of Health Care Services** | State of California seal |
|  |  |

## **AGREEMENT FOR USE OF DATA CONTAINING**

## **INDIVIDUAL AND PROVIDER SPECIFIC INFORMATION**

**NOTE:** Requestors must initial every page, date and sign this Data Use Agreement if you intend to mail the hard copy instead of DocuSign.

In order to secure data that resides in the California Department of Health Care Services (“DHCS”) system of records, and in order to ensure the integrity, security, and confidentiality of information maintained by DHCS, and to permit appropriate disclosure and use of such data as permitted by law, DHCS and       enter into this Agreement to comply with the following specific sections. This Agreement shall be binding on any successors to the parties.

1. This Agreement is by and between DHCS, and       hereinafter termed “User” and is applicable to the research project,       [insert name from application].

1. This Agreement addresses the conditions under which DHCS will disclose and the

User will obtain and use the data specified in ***Exhibit A*** - *Application to Obtain Protected DHCS Data for Research* and in ***Exhibit B –*** *Data Description Table.* This Agreement supplements any agreements between the parties with respect to the use of data from the files specified in ***Exhibits A*** and ***B*** and preempts and overrides any contrary instructions, directions, agreements, or other understanding in or pertaining to any grant award or other prior communication from the DHCS or any of its components with respect to the data specified herein. Whenever a requirement in this Agreement is more stringent with respect to the protection of DHCS data than any other requirement of this Agreement or applicable laws and regulations, the more stringent requirement shall apply. Further, the terms of this Agreement can be changed only by a written modification to this Agreement or by the parties entering into a new agreement. The parties agree further that instructions or interpretations issued to the User concerning this Agreement or the data specified herein, shall not be valid unless issued in writing by the DHCS signatory to this Agreement shown in Section 29.

1. The parties mutually agree that the following specified exhibits are part of this

Agreement:

* ***Exhibit A - Application to Obtain Protected DHCS Data for Research***
* ***Exhibit B - Data Description Table***
* ***Exhibit C - Data Security Requirements***
* ***Exhibit D - Notification of Breach***
1. This Agreement shall not take effect unless the User has obtained an approval

letter from the Committee for The Protection of Human Subjects of the California Health and Human Services Agency for the research project set forth in ***Exhibit A***. User is responsible for obtaining approval that will be in effect for the entire period of time covered by this Agreement.

5. The parties mutually agree that DHCS retains all ownership rights to the data referred to in this Agreement, and that the User does not obtain any right, title, or interest in any of the data furnished by DHCS.

1. The term “DHCS data” shall include:
2. “Protected Health Information” or “PHI.” PHI means any information, whether oral or recorded, in any form or medium that relates to the past, present, or future physical or mental condition of an individual, the provision of health and dental care to an individual, or the past, present, or future payment for the provision of health and dental care to an individual; and that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. PHI shall have the meaning given to such term under HIPAA and HIPAA regulations, as the same may be amended from time to time.

(b) “Personal Confidential Information” or “PCI.” PCI means any information that

identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, medical or employment history, and statements made by, or attributed to, the individual. It also includes health program payment or operations records that identify an individual, and health insurance information in combination with the individual’s name.

1. The term “Security Incident” means the attempted or successful unauthorized access, use,

 disclosure, modification, or destruction of PHI, or PCI utilized pursuant to this Agreement; or

 interference with system operations in an information system that processes, maintains or

 stores PHI or PCI.

8. The parties mutually agree that the following named individual is designated as “Custodian” of the file(s) on behalf of the User and will be responsible for the observance of all conditions of use and for establishment and maintenance of security arrangements as specified in this Agreement to prevent unauthorized use. The User agrees to notify the DHCS point of contact designated in Section 9 within fifteen (15) days of any change of custodianship. The parties mutually agree that DHCS may disapprove the appointment of a custodian or may require the appointment of a new custodian at any time.

(Name of Custodian of File(s) - Typed or Printed)

(Title/Component)

(Company/Organization)

(Address)

(City/State/ZIP Code)

(Phone Number and E-Mail Address)

9. The parties mutually agree that the Administrator of the DHCS Data and Research Committee will be designated as “point-of-contact” for the Agreement on behalf of DHCS.

 Data and Research Committee Administrator

 DHCS Data and Research Committee

(916) 440-7617

DHCSDRC@dhcs.ca.gov

10. The DHCS data listed in ***Exhibits A and B*** is/are covered under this Agreement.

The User represents and warrants, and in furnishing the data specified in ***Exhibits A and B*** DHCS relies upon such representation and warranty, that such data will be used solely for the purposes as described in ***Exhibit A*** and as presented to the California Health and Human Services Agency’s Committee for Protection of Human Subjects (CPHS).

The User represents and warrants further that the facts and statements made in any study or research protocol or project plan described in ***Exhibit A*** are complete and accurate. Further, the User represents and warrants that said study protocol(s) or project plans, as have been approved by DHCS and CPHS, or other appropriate entity as DHCS may determine, represent the total use(s) to which the data specified in ***Exhibits A and B*** will be put.

The User represents and warrants further that, except as DHCS shall authorize in writing, the User shall not disclose, release, reveal, show, sell, rent, lease, loan, or otherwise grant access to the data covered by this Agreement to any person, company or organization. The User agrees that, within the User organization, access to the data covered by this Agreement shall be limited to the minimum number of individuals necessary to achieve the purpose stated in ***Exhibit A*** and to those individuals on a need-to-know basis only.

11. The parties mutually agree that the expiration date for retention of the aforesaid data (and/or any derivative files, including any file that maintains or continues identification of individuals) will be the date designated by DHCS in Section 25. Requests for extension of the expiration date may be granted by DHCS for a one year period. Requests for extension must be made in writing (including justification for the request) by the User within the 60 days prior to the expiration date. Final approval, if given, is contingent upon renewal of the approval from CPHS.

12. The User agrees to notify DHCS within 30 days of the completion of the purpose specified in Section 10 if the purpose is completed before the aforementioned expiration date. Upon such completion or expiration date, whichever occurs sooner, the User shall destroy all electronic data files with DHCS data by wiping such data using the Gutmann or U.S. Department of Defense (DoD) 5220.22M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission of the DHCS Information Security Office. The User shall destroy all paper documents with DHCS data by using a confidential method of destruction, such as crosscut shredding and pulverizing or contracting with a company that specializes in confidential destruction of documents. The User shall certify the destruction of the data in writing within 30 days of the destruction. A statement certifying this action must be sent to the DHCS point-of-contact listed in Section 9. The provisions of this Agreement governing the privacy and security of the PHI and PCI shall remain in effect until all PHI and PCI is destroyed and DHCS receives a certificate of destruction from User. The User agrees that no data from DHCS records, any parts or copies thereof, including files derived from DHCS records (electronic, hardcopy or otherwise), shall be retained when the data are destroyed unless authorization in writing for the retention of such data has been received from the person designated in Section 28. The only exception is data that has been de-identified by the User as defined in 45 CFR Parts 164.514(a) and 164.514(b) of the Health Insurance Portability and Accountability Act (HIPAA) privacy regulations, as amended. The User acknowledges that stringent adherence to the aforementioned expiration date is required.

13. The User agrees to establish and maintain appropriate administrative, technical, and physical safeguards to protect the confidentiality of the data and to prevent unauthorized use or access to it. The safeguards shall provide a level and scope of security that is not less than the level and scope of security established in 45 CFR, parts 160, 162 and 164 of HIPAA Privacy and Security Regulations, as amended. User shall also provide a level and scope of security that is at least comparable to that established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III – Security of Federal Automated Information. In addition, User agrees to comply with the specific security controls enumerated in ***Exhibit C*** – *Data Security Requirements* of this Data Use Agreement. The User also agrees to ensure that any agents, including a subcontractor to whom it provides the DHCS data, agree to the same privacy and security safeguards for confidential information that apply to the User with respect to such information.

14. The User agrees that any findings, listings, or information derived from the data specified in ***Exhibits A and B***, may not be released unless such findings, listings, or information comply with the standards for de-identification of individual beneficiary data established in 45 CFR Parts 164.514(a) and 164.514(b) of the HIPAA Privacy regulations, as amended. The User also agrees to provide DHCS with annual reports that provide the results of the research accomplished under this Agreement, whether published or unpublished, to discuss such results with a representative of DHCS, and to send copies or reprints of all published findings resulting from the research covered by this Data Use Agreement to DHCS at the address below:

 Department of Health Care Services

Information Management Division, MS 0021

P.O. Box 997413

Sacramento, CA 95899-7413

Or via email to:

DHCSDRC@dhcs.ca.gov

15. The User agrees that, absent express written authorization from the person designated in Section 28 to do so, the User shall make no attempt to link records included in the data or data file(s) specified in ***Exhibits A or B*** to any other identifiable source of information. This includes attempts to link to other DHCS data file(s). The inclusion of linkage of specific files specified in ***Exhibit B*** is considered express written authorization from DHCS.

1. The User understands and agrees that User may not reuse original or derivative data

without prior written approval from the person designated in Section 29. The only exception is data that has been de-identified by the User as defined in 45 CFR Parts 164.514(a) and 164.514(b) of the HIPAA Privacy regulations.

17. The User acknowledges that in addition to the requirements of this Data Use

Agreement, it must also abide by the privacy and disclosure laws and regulations under 45 CFR, Parts 160, 162 and 164 of the HIPAA privacy and security regulations, Section 14100.2 of the California Welfare & Institutions Code, and Confidentiality of Alcohol and Drug Abuse Patient (ADP) Records law, 42 CFR Part 2, as well as any other applicable state or federal law or regulation. User acknowledges that 42 CFR Section 2.53(d) limits the use and re-disclosure of the information provided by DHCS: Patient identifying information disclosed under 42 CFR Part 2 may be disclosed only back to the program from which it was obtained and used only to carry out an audit or evaluation purpose or to investigate or prosecute criminal or other activities, as authorized by an appropriate court order entered under 42 CFR §2.66.. The User also agrees to ensure that any agents, including a subcontractor to whom it provides the DHCS data, agree to the same restrictions and conditions that apply to the User with respect to such information. Any such agents, including subcontractors, must be named in ***Exhibit A***.

18. The User agrees that no attempt will be made to unencrypt or otherwise re-identify any

encrypted person-level data in the file(s). Further, unless expressly approved by DHCS and the Committee for the Protection of Human Subjects of the California Health and Human Services Agency, the User agrees not to attempt to identify or contact any specific individual whose record is included in the data.

19. The User agrees to report to DHCS any use or disclosure of the information not

provided for by this Data Use Agreement of which it becomes aware, immediately upon discovery, and to take further action regarding the use or disclosure as specified in ***Exhibit D*** – *Notification of Breach* of this Data Use Agreement.

20. User agrees to train and use reasonable measures to ensure compliance with the requirements of this Agreement by employees who assist in the performance of functions or activities under this Agreement and use or disclose DHCS data, and to discipline such employees who intentionally violate any provisions of this Agreement, including by termination of employment. In complying with the provisions of this section, User shall observe the following requirements:

1. User shall provide information privacy and security training, at least annually, at

its own expense, to all its employees who assist in the performance of functions or activities under this Agreement and use or disclose DHCS data; and

1. User shall require each employee who receives information privacy and security

training to sign a certification, indicating the employee’s name and the date on

which the training was completed.

21. From time to time, DHCS may, upon prior written notice and at mutually convenient times, inspect the facilities, systems, books and records of User to monitor compliance with this Agreement. User shall promptly remedy any violation of any provision of this Agreement and shall certify the same to the DHCS Privacy Officer in writing. The fact that DHCS inspects, or fails to inspect, or has the right to inspect, User’s facilities, systems and procedures does not relieve User of its responsibility to comply with this Agreement.

22. The User acknowledges that criminal penalties under 45 CFR, parts 160, 162 and 164 of the HIPAA privacy and security regulations, and Section 14100.2 of the California Welfare & Institutions Code, including possible fines and imprisonment, may apply with respect to any disclosure of information in the data or data file(s) that is inconsistent with the terms of this Agreement. The User further acknowledges that criminal penalties under the Confidentiality of Medical Information Act (California Civil Code § 56) may apply if it is determined that the User, or any individual employed or affiliated therewith, knowingly and willfully obtained the data or data file(s) under false pretenses.

23. By signing this Agreement, the User agrees to abide by all provisions set out in this Agreement, and in ***Exhibits C and D*** for protection of the data and data file(s) specified in ***Exhibits A and B***, and acknowledges having received notice of potential criminal, administrative, or civil penalties for violation of the terms of the Agreement. Further, the User agrees that any material violations of the terms of this Agreement or any of the laws and regulations governing the use of DHCS data may result in permanent denial of access to DHCS data.

24. The User agrees to pay all costs incurred by DHCS in regards to this request, including, but not limited to, staff time and data processing charges.

25. Expiration Date. The expiration date of this agreement shall be one year from the date the Data Research Committee Chair signs section 29, unless an extension is granted as specified in Section 11.

26. Termination for Cause. Upon DHCS’ knowledge of a material breach or violation of this Agreement by User, DHCS may provide an opportunity for User to cure the breach or end the violation and may terminate this Agreement if User does not cure the breach or end the violation within the time specified by DHCS. DHCS may terminate this Agreement immediately if User has breached a material term and DHCS determines, in its sole discretion, that cure is not possible or available under the circumstances. Upon termination of this Agreement, User must destroy all PHI and PCI in accordance with Section 12, above. The provisions of this Agreement governing the privacy and security of the PHI and PCI shall remain in effect until all PHI and PCI is destroyed and DHCS receives a certificate of destruction from User.

27. The Custodian, as named in Section 8, hereby acknowledges his/her appointment as Custodian of the aforesaid data on behalf of the User, and agrees in a representative capacity to comply with all of the provisions of this Agreement on behalf of the User.

(Name of Custodian of File(s) - Typed or Printed)

(Title/Component)

(Signature) (Date)

28. On behalf of the User, the undersigned individual hereby attests that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.

(Name - Typed or Printed)

(Title/Component)

(Company/Organization)

(Address)

(City/State/ZIP Code)

(Phone Number and E-Mail Address)

(Signature) (Date)

29. *This section is to be completed by DHCS.*

On behalf of DHCS the undersigned individual hereby attests that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.

Linette Scott, MD, MPH

(Name of DHCS Representative)

Chair, Data and Research Committee

(Title/Component)

(Signature) (Date)