CA

97394 Applications for Research Identifiable Data Through the Enclave

(a)

Data Application. To request access to research identifiable data through the enclave, an individual or organization must electronically submit an application through the Department's website with all of the following: (1) Designation as a new application or a supplemental application. If a supplemental application, the request number of the previously approved project. (2) Name of the data applicant, and whether an individual or type of organization. (3) Whether the data applicant submits data to the program. (4) Name, title, phone number, business address, and email address of the applicant, if an individual, or the authorized representative. (5) Whether the applicant has applied for data from the Department previously, and if applicable, the associated request number(s) and project title(s). (6) If the point of contact for the application is different than the data applicant, the name, title, business address, phone number and email address of the point of contact. (7) Project title. (8) A detailed description of the requested program data to allow the Department to determine whether the data exists, or whether it can be created. This includes the time period of data requested, a list of each confidential data element desired and an explanation of why the data applicant needs each confidential data element. (9) If the applicant is requesting access to Medi-Cal data, how the use of the data will contribute to the project. (10) A description of the

research project, the anticipated use of the data, and how the project offers significant opportunities to achieve program goals. This includes a description of public data products that may be created with research identifiable data and how these products will be disclosed. (11) Anticipated length of time the data applicant will need the confidential data in the enclave. (12) List of any data from outside the program which the data applicant wants to use or link with the confidential data and the anticipated use of those data. (13) List of all individuals, contractors and other third parties, who are anticipated to use, control, observe, transmit or store confidential data and the physical location(s) from which they may work. This includes each individual's, contractor's or other third parties' name, organization, phone number, business address, email address, title, and role regarding the data (such as part of the data analysis team or the information technology team). This includes the data applicant if an individual, or the authorized representative. (14) If the applicant is working with a contractor or other third party, a copy of any contract(s) or agreement(s) between the collaborating entities. (15) Regarding the applicant, if an individual, or the authorized representative, a description and supporting documentation of this individual's expertise with privacy protection and with the analysis of large sets of confidential information. (16) History of data breaches: A description of any data breaches or other similar incidents in which PII was misused or improperly disclosed in the past seven (7) years, which the applicant or the authorized representative, if any, caused or was responsible for; and corrective measures, if any, taken after such incidents. (17) Convictions/Civil Actions: For the applicant and the authorized representative, if any, a disclosure of criminal convictions or substantiated violations of law regarding fraud, theft, data breach, data misuse, or related offenses, in the past seven (7) years. This includes civil or administrative penalties, civil judgements, or disciplinary actions. (18) The

security measures to protect against the unauthorized disclosure of confidential data, such as physical security for the physical location(s) where access will take place, controls limiting who can view the data, and background screening for individuals who will access the data. This includes the specific data access method for any contractors or other third parties. (19) The applicant's security plan for protecting access to the confidential data. This includes an acknowledgment of having read the data security standards and requirements in section 97406, and a description of how the data security standards and requirements in section 97406(b) will be met. (20) Detailed information explaining how the requested data is the minimum amount of confidential data required for the project. (21) A statement by the data applicant agreeing to make the research from the research project available to the Department. (22) A copy of the applicant's draft or submitted application to the Committee for the Protection of Human Subjects (23) The following information is required for access to requested data through the enclave. (A) The volume of data the applicant is intending to upload into the enclave. (B) The individual responsible for uploading data to the enclave. (C) For each individual who will access the data, the type of access the applicant wants for the individual, and any additional software or tools the applicant wants available for the individual in the enclave. (24) Signature of the data applicant(s), if an individual or individuals, or the authorized representative, and the date of signature. This signature shall certify that the information provided in the application is true and correct.

(1)

Designation as a new application or a supplemental application. If a supplemental application, the request number of the previously approved project.

(2)

Name of the data applicant, and whether an individual or type of organization.

(3)

Whether the data applicant submits data to the program.

(4)

Name, title, phone number, business address, and email address of the applicant, if an individual, or the authorized representative.

(5)

Whether the applicant has applied for data from the Department previously, and if applicable, the associated request number(s) and project title(s).

(6)

If the point of contact for the application is different than the data applicant, the name, title, business address, phone number and email address of the point of contact.

(7)

Project title.

(8)

A detailed description of the requested program data to allow the Department to determine whether the data exists, or whether it can be created. This includes the time period of data requested, a list of each confidential data element desired and an explanation of why the data applicant needs each confidential data element.

(9)

If the applicant is requesting access to Medi-Cal data, how the use of the data will contribute to the project.

(10)

A description of the research project, the anticipated use of the data, and how the project offers significant opportunities to achieve program goals. This includes a description of public data products that may be created with research identifiable data

and how these products will be disclosed.

(11)

Anticipated length of time the data applicant will need the confidential data in the enclave.

(12)

List of any data from outside the program which the data applicant wants to use or link with the confidential data and the anticipated use of those data.

(13)

List of all individuals, contractors and other third parties, who are anticipated to use, control, observe, transmit or store confidential data and the physical location(s) from which they may work. This includes each individual's, contractor's or other third parties' name, organization, phone number, business address, email address, title, and role regarding the data (such as part of the data analysis team or the information technology team). This includes the data applicant if an individual, or the authorized representative.

(14)

If the applicant is working with a contractor or other third party, a copy of any contract(s) or agreement(s) between the collaborating entities.

(15)

Regarding the applicant, if an individual, or the authorized representative, a description and supporting documentation of this individual's expertise with privacy protection and with the analysis of large sets of confidential information.

(16)

History of data breaches: A description of any data breaches or other similar incidents in which PII was misused or improperly disclosed in the past seven (7) years, which the applicant or the authorized representative, if any, caused or was responsible for; and corrective measures, if any, taken after such incidents.

(17)

Convictions/Civil Actions: For the applicant and the authorized representative, if any, a disclosure of criminal convictions or substantiated violations of law regarding fraud, theft, data breach, data misuse, or related offenses, in the past seven (7) years. This includes civil or administrative penalties, civil judgements, or disciplinary actions.

(18)

The security measures to protect against the unauthorized disclosure of confidential data, such as physical security for the physical location(s) where access will take place, controls limiting who can view the data, and background screening for individuals who will access the data. This includes the specific data access method for any contractors or other third parties.

(19)

The applicant's security plan for protecting access to the confidential data. This includes an acknowledgment of having read the data security standards and requirements in section 97406, and a description of how the data security standards and requirements in section 97406(b) will be met.

(20)

Detailed information explaining how the requested data is the minimum amount of confidential data required for the project.

(21)

A statement by the data applicant agreeing to make the research from the research project available to the Department.

(22)

A copy of the applicant's draft or submitted application to the Committee for the Protection of Human Subjects

(23)

The following information is required for access to requested data through the enclave. (A) The volume of data the applicant is intending to upload into the enclave. (B) The individual responsible for uploading data to the enclave. (C) For each individual who will access the data, the type of access the applicant wants for the individual, and any additional software or tools the applicant wants available for the individual in the enclave.

(A)

The volume of data the applicant is intending to upload into the enclave.

(B)

The individual responsible for uploading data to the enclave.

(C)

For each individual who will access the data, the type of access the applicant wants for the individual, and any additional software or tools the applicant wants available for the individual in the enclave.

(24)

Signature of the data applicant(s), if an individual or individuals, or the authorized representative, and the date of signature. This signature shall certify that the information provided in the application is true and correct.

(b)

Other Mandatory Reasons for Denial. In addition to section 97388, the Department shall deny an application under this section, in whole or in part, if the Department determines that: (1) The proposed use of the confidential data is not for a research project; (2) The research project does not offer significant opportunities to achieve program goals; (3) The Data Release Committee does not recommend project approval; (4) The data applicant is unable to provide documentation that the Committee for the Protection of Human Subjects has approved the project,

pursuant to subdivision (t) of Section 1798.24 of the Civil Code; (5) The applicant, if an individual, or the authorized representative does not have documented expertise with privacy protection and with the analysis of large sets of confidential information; or (6) The applicant does not agree to make its research using the confidential data available to the Department.

(1)

The proposed use of the confidential data is not for a research project;

(2)

The research project does not offer significant opportunities to achieve program goals;

(3)

The Data Release Committee does not recommend project approval;

(4)

The data applicant is unable to provide documentation that the Committee for the Protection of Human Subjects has approved the project, pursuant to subdivision (t) of Section 1798.24 of the Civil Code;

(5)

The applicant, if an individual, or the authorized representative does not have documented expertise with privacy protection and with the analysis of large sets of confidential information; or

(6)

The applicant does not agree to make its research using the confidential data available to the Department.