97398 Researcher Applications for the Direct Transmission of Confidential Data

(a)

Data Application. To request direct transmission of confidential data other than standardized limited datasets, a researcher, who has overall responsibility and authority over the research project, 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, title, phone number, business mailing address, and email address of the data applicant(s). (3) Documentation establishing that the applicant is a researcher as defined in this Article. (4) Name of the organization, if any, with which the researcher is affiliated; and the name of individuals or organizations, if any, for which the researcher desires to conduct research with the requested confidential data. (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) Whether the applicant or the affiliated organization submits data to the program. (8) Project title. (9) 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. (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 confidential data and how these products will be disclosed. (11) If the applicant is requesting access to Medi-Cal data, how the use of the data will contribute to the project. (12) Explanation of why the data applicant needs direct transmission of the confidential data instead of accessing the data through the enclave. (13) Anticipated length of time the confidential data will be needed to accomplish the project. (14) 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. (15) 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. (16) If the applicant is working with a contractor or other third party, a copy of the contract(s) or agreement(s) between the collaborating entities. (17) A description and supporting documentation of the data applicant's expertise with privacy protection, with the analysis of large sets of confidential information, and with data security and the protection of large sets of confidential information. (18) 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 caused or was responsible for; and corrective measures,

if any, taken after such incidents. (19) Convictions/Civil Actions: A disclosure of the applicant's 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. (20) The applicant's data security plan for protecting the confidential data, with supporting documentation. This includes an acknowledgment of having read the data security standards and requirements in section 97406, a description of how the data security standards and requirements in section 97406 will be met and the specific data access method for any contractors or other third parties. (21) Detailed information explaining how the requested data is the minimum amount of confidential data required for the project. (22) Name, phone number, and email address of the individual who will be responsible for information security of the confidential data. (23) A statement by the applicant agreeing to make the research from the research project available to the Department. (24) A copy of the applicant's draft or submitted application to the Committee for the Protection of Human Subjects. (25) Signature of the data applicant(s), 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, title, phone number, business mailing address, and email address of the data applicant(s).

(3)

Documentation establishing that the applicant is a researcher as defined in this Article.

(4)

Name of the organization, if any, with which the researcher is affiliated; and the name of individuals or organizations, if any, for which the researcher desires to conduct research with the requested confidential data.

(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)

Whether the applicant or the affiliated organization submits data to the program.

(8)

Project title.

(9)

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.

(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 confidential data and how these products will be disclosed.

(11)

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

contribute to the project.

(12)

Explanation of why the data applicant needs direct transmission of the confidential data instead of accessing the data through the enclave.

(13)

Anticipated length of time the confidential data will be needed to accomplish the project.

(14)

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.

(15)

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.

(16)

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

(17)

A description and supporting documentation of the data applicant's expertise with privacy protection, with the analysis of large sets of confidential information, and with data security and the protection of large sets of confidential information.

(18)

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 caused or was responsible for; and corrective measures, if any, taken after such incidents.

(19)

Convictions/Civil Actions: A disclosure of the applicant's 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.

(20)

The applicant's data security plan for protecting the confidential data, with supporting documentation. This includes an acknowledgment of having read the data security standards and requirements in section 97406, a description of how the data security standards and requirements in section 97406 will be met and the specific data access method for any contractors or other third parties.

(21)

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

(22)

Name, phone number, and email address of the individual who will be responsible for information security of the confidential data.

(23)

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

(24)

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

(25)

Signature of the data applicant(s), 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 applicant is not a researcher; (2) The proposed use of the confidential data is not for a research project; (3) The research project does not offer significant opportunities to achieve program goals; (4) The Data Release Committee did not recommend project approval; (5) 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; (6) The data applicant does not have documented expertise with privacy protection, with the analysis of large sets of confidential data, and with data security and the protection of large sets of confidential data; or (7) The data applicant does not agree to make its research using the confidential data available to the Department.

(1)

The applicant is not a researcher;

(2)

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

(3)

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

(4)

The Data Release Committee did not recommend project approval;

(5)

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;

(6)

The data applicant does not have documented expertise with privacy protection, with the analysis of large sets of confidential data, and with data security and the protection of large sets of confidential data; or

(7)

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