

## **97396 Applications for the Direct Transmission of Standardized Limited Datasets**

### **(a)**

Data Application. To request direct transmission of a standardized limited dataset 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) Identification of the standardized limited dataset the data applicant wants, the time period of data, and a description of how the project meets the purposes specified by the Department for the standardized limited dataset. This includes an explanation of why the data applicant needs each confidential data element desired from the standardized limited dataset. (9) A description of the data use, and how the purpose is consistent with program goals. This includes a description

of any public data products that may be created with the standardized limited dataset and how these products will be disclosed. (10) If the applicant is requesting access to Medi-Cal data, how the use of the data will contribute to the project. (11) Explanation why the data applicant needs direct transmission of the confidential data instead of accessing the data through the enclave. (12) Anticipated length of time the confidential data will be needed to accomplish the use. (13) 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. (14) 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. (15) 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. (16) 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. (17) 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. (18) 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. (19) The applicant's 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. (20) Name, phone number, and email address of the individual who will be responsible for information security of the confidential data. (21) 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)**

Identification of the standardized limited dataset the data applicant wants, the time period of data, and a description of how the project meets the purposes specified by the Department for the standardized limited dataset. This includes an explanation of why the data applicant needs each confidential data element desired from the standardized limited dataset.

**(9)**

A description of the data use, and how the purpose is consistent with program goals. This includes a description of any public data products that may be created with the standardized limited dataset and how these products will be disclosed.

**(10)**

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

**(11)**

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

**(12)**

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

**(13)**

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.

**(14)**

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.

**(15)**

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.

**(16)**

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.

**(17)**

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.

**(18)**

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.

**(19)**

The applicant's 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.

**(20)**

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

**(21)**

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)**

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 inconsistent with the purposes specified by the Department for the requested standardized limited dataset; (2) 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; (3) The Data Release Committee did not recommend project approval; or (4) The application requests a standardized limited dataset that contains identifiable information for any individual or organization who furnishes, bills, or is paid for health care in the normal course of business.

**(1)**

The proposed use of the confidential data is inconsistent with the purposes specified by the Department for the requested standardized limited dataset;

**(2)**

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;

**(3)**

The Data Release Committee did not recommend project approval; or

**(4)**

The application requests a standardized limited dataset that contains identifiable information for any individual or organization who furnishes, bills, or is paid for health care in the normal course of business.