CA

97400 State Agency Applications for Confidential Data

(a)

Data Application. For state agencies requesting confidential data, a state agency 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 state agency. (3) Whether the state agency submits data to the program. (4) Name, title, phone number, business mailing address, and email address of the authorized representative for the state agency. (5) Project title. (6) 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 state agency needs each confidential data element. (7) An explanation why the state agency wants the data, including a description of the data use, goals, how the data will be used for purposes consistent with the program, and how the confidential data is necessary for the state agency to perform its constitutional or statutory duties. This also includes a description of public data products that may be created with confidential data, and how these products will be disclosed. (8) If the state agency is requesting access to Medi-Cal data, how the use of the data will contribute to the project. (9) How the state agency wants the data, such as through the enclave or by direct

transmission. If by direct transmission, an explanation why the state agency needs direct transmission of the confidential data instead of accessing the data through the enclave. (10) Anticipated length of time the confidential data will be needed to accomplish the project. (11) List of any data from outside the program which the state agency wants to use or link with the confidential data and the anticipated use of those data. (12) 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 authorized representative. (13) If the state agency is working with a contractor or other third party, a copy of the contract(s) or agreement(s) between the collaborating entities. (14) 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 state agency or the authorized representative, if any, caused or was responsible for; and corrective measures, if any, taken after such incidents. (15) Convictions/Civil Actions: For the state agency 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. (16) Data Security: (A) If requesting confidential data through the enclave, 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, background screening for individuals who will access the data, the state

agency's security plan for protecting access to the confidential data, a description of how the data security standards and requirements in section 97406(b) will be met, and an acknowledgment of having read the data security standards and requirements in section 97406. This includes the specific data access method for any contractors or third parties; or (B) If requesting direct transmission of confidential data, the state agency'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 name, phone number, and email address of the individual who will be responsible for information security of the confidential data. This includes the specific data access method for any contractors or third parties. (17) The following information is required for access to requested data through the enclave. (A) The volume of data the state agency 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. (18) Signature of the authorized representative of the state agency, 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 state agency.

(3)

Whether the state agency submits data to the program.

(4)

Name, title, phone number, business mailing address, and email address of the authorized representative for the state agency.

(5)

Project title.

(6)

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 state agency needs each confidential data element.

(7)

An explanation why the state agency wants the data, including a description of the data use, goals, how the data will be used for purposes consistent with the program, and how the confidential data is necessary for the state agency to perform its constitutional or statutory duties. This also includes a description of public data products that may be created with confidential data, and how these products will be disclosed.

(8)

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

(9)

How the state agency wants the data, such as through the enclave or by direct transmission. If by direct transmission, an explanation why the state agency needs direct transmission of the confidential data instead of accessing the data through the enclave.

(10)

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

(11)

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

(12)

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 authorized representative.

(13)

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

(14)

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 state agency or the authorized representative, if any, caused or was responsible for; and corrective measures, if any, taken after such incidents.

(15)

Convictions/Civil Actions: For the state agency 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.

(16)

Data Security: (A) If requesting confidential data through the enclave, 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, background screening for individuals who will access the data, the state agency's security plan for protecting access to the confidential data, a description of how the data security standards and requirements in section 97406(b) will be met, and an acknowledgment of having read the data security standards and requirements in section 97406. This includes the specific data access method for any contractors or third parties; or (B) If requesting direct transmission of confidential data, the state agency'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 name, phone number, and email address of the individual who will be responsible for information security of the confidential data. This includes the specific data access method for any contractors or third parties.

(A)

If requesting confidential data through the enclave, 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, background screening for individuals who will access the data, the state agency's security plan for protecting access to the confidential data, a description of how the data security standards and requirements in section 97406(b) will be met, and an acknowledgment of having read the data security standards and requirements in section 97406. This includes the specific data access method for any contractors or third parties; or

(B)

If requesting direct transmission of confidential data, the state agency'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 name, phone number, and email address of the individual who will be responsible for information security of the confidential data. This includes the specific data access method for any contractors or third parties.

(17)

The following information is required for access to requested data through the enclave. (A) The volume of data the state agency 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 state agency 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.

(18)

Signature of the authorized representative of the state agency, 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 confidential data is not necessary for the state agency to perform its constitutional or statutory duties; or (2) The state agency's proposed use of the confidential data is incompatible with a purpose for which the data was collected.

(1)

The confidential data is not necessary for the state agency to perform its constitutional or statutory duties; or

(2)

The state agency's proposed use of the confidential data is incompatible with a purpose for which the data was collected.