DRAFT

HPD Data Use, Access, and Release Regulations

12~~6~~/15~~2~~/2023

Proposed changes are shown in double underline and ~~double strikeout~~.

Article 8. Data Use, Access, and Release

§97380. Additional Definitions for this Article

In addition to the definitions in section 93700, the following definitions apply to this article:

(a) “Aggregated data” means that the data does not have any record-level information about individuals, and only has collective data that relates to a group or category of services or individuals.

(b) “Authorized representative” means, if the data applicant is not an individual, the individual who will have overall responsibility and authority over the requested program data on behalf of the data applicant.

(c) “Confidential Data” means program data that has PII or record-level information about patients or individual consumers. This includes aggregated data that is identifiable.

(d) “Custom Limited Datasets” are datasets other than standardized limited datasets, with confidential data that do not include any of the direct personal identifiers listed in Section 164.514(e) of Title 45 of the Code of Federal Regulations.

(ed) “Data Applicant(s)” or “Applicant(s)” means any individual, group of individuals, or organization that submits an application for program data under this Article. For Research Identifiable applications, sections 97394 and 97398, data applicant may be used interchangeably with Principal Investigator (PI) and Co-Principal Investigator (Co-PI).

(fe) “Data Product” means information derived, in whole or in part, from program data, including, but not limited to, visualizations, summary data tables, report findings, listings, or publications.

(gf) “Data Release Committee” means the committee established pursuant to Health and Safety Code section 127673.84.

(hg) “Data User” means a data applicant that has been approved for program data under this Article.

(ih) “Direct Transmission” means the Department sending copies of program data outside the enclave directly to an individual or organization.

(ji) “Enclave” is the program's secure online data access environment, required by Health and Safety Code Section 127673.82(d), through which individuals will be able to remotely observe, use, or control program data. (k) “Personally Identifiable Information” or “PII” is any information that can be reasonably used to distinguish or trace an individual’s identity, either alone or when combined with other information.

(l) “Program Data” means all information created, obtained, or maintained by the program. This includes confidential data.

(m) “Program Goals” means the purposes stated for the program in Health and Safety Code sections 127671 and 127673.5(a).

(n) “Public data products” mean data products created by data users that are intended for disclosure publicly or to individuals not approved for program data under an approved data application.

(o) “Record-level” means information about a single individual.

(p) “Research” means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge as stated in Section 164.501 of Title 45 of the Code of Federal Regulations.

(q) “Research Identifiable Data” means confidential data with the direct personal identifiers listed in Section 164.514(e) of Title 45 of the Code of Federal Regulations.

(r) “Researcher” means an individual, who routinely conducts health care or health care related research, and meets all of the following criteria:

(1) Has possession of a bachelor’s degree or higher-level degree in a field that conducts research. These fields include, but are not limited to, physical sciences, life sciences, social sciences, and medical sciences;
(2) Is research-affiliated with a research entity including, but not limited to, public and private universities and medical schools, as well as other organizations that conduct health and social science research, or public departments and agencies; and
(3) Has research experience at an accredited university or college, research entity, or public agency.

(s) “Standardized limited datasets” are datasets developed by the Department with confidential data that do not include any of the direct personal identifiers listed in Section 164.514(e) of Title 45 of the Code of Federal Regulations and have the minimum necessary personal information for types of purposes specified by the Department.

(t) “State agency” means every state office, officer, department, division, bureau, board, commission or other state agency of the executive branch of the state government of California.

(u) “Supplemental applications” are applications related to a previously approved project.

Note: Authority cited: Section 127673, Health and Safety Code. Reference: Sections 127671, 127673.5, 127673.8, 127673.81, 127673.82, 127673.83, and 127673.84, Health and Safety Code.

§97382. Eligibility for Program Data

(a) Non-Confidential Program Data. Any individual or organization may request program data that does not contain any confidential data by submitting an application pursuant to section 97390.

(b) Standardized Limited Datasets via the Enclave. Any individual or organization may request enclave access to Standardized limited datasets by submitting an application pursuant to section 97392.

(c) Custom Limited Datasets via the Enclave. Any individual or organization may request enclave access to Custom Limited Datasets by submitting an application pursuant to section 97393.

(dc) Research Identifiable Data Through the Enclave. Any individual or organization may request enclave access to research identifiable data by submitting an application pursuant to section 97394.

(ed) Direct Transmission of Standardized Limited Datasets. Any individual or organization may request direct transmission of a standardized limited dataset, ~~either in whole or in part,~~ by submitting an application pursuant to section 97396.

(fe) Direct Transmission of Confidential Data. A researcher may request direct transmission of confidential data other than standardized limited datasets, by submitting an application pursuant to section 97398.

(gf) State Agency Requests for Confidential Data. In addition to the above, a state agency may request confidential data by submitting an application pursuant to section 97400.

Note: Authority cited: Section 127673, Health and Safety Code. Reference: Sections 127673.81, 127673.82, and 127673.83, Health and Safety Code.

§97384. Application Fees

(a) An individual or organization, except state agencies, submitting an application for program data under this Article shall pay the application fee set by the Department.

(b) The application fee of $100 shall be submitted at the time the individual or organization submits its new data application or supplemental application, and no application shall be considered complete unless accompanied by the required fee. The paid fee shall be applied to the total cost for the data if the application is approved. The application fee is non-refundable.

Note: Authority cited: Section 127673, Health and Safety Code. Reference: Sections 127673.81, 127673.82, and 127674, Health and Safety Code.

§97386. Review of Applications

When reviewing applications for program data submitted under this Article, the Department may do any of the following to make its decision:

(a) Seek further information from the applicant, including, but not limited to, documents or evidence verifying information;
(b) Seek input or recommendations from the Data Release Committee, even if not required by this Article; or
(c) Seek input or information from other sources, including, but not limited to, the public, regulatory bodies, other state agencies, the Health Care Payments Data Program Advisory Committee, or the sources of the requested data.

Note: Authority cited: Section 127673, Health and Safety Code. Reference: Sections 127673.8, 127673.81, 127673.82, 127673.83, and 127673.84, Health and Safety Code.

§97388. General Reasons to Deny Applications

(a) This section applies to all applications for program data submitted to the Department under this Article. There may be specific restrictions or requirements depending on the type of data request.

(b) Mandatory Reasons for Denial. The Department shall deny an application, in whole or in part, if the Department determines that:

(1) State or federal law prohibits the disclosure of the data;

(2) The agreement through which the Department obtained the requested data prohibits disclosure of the data;

(3) Disclosure of the data would create an unreasonable risk to individual privacy or safety;

(4) The proposed use of the data is inconsistent with program goals;

(5) Regarding applications for confidential data:

(A) The applicant does not need the requested confidential data for its proposed use;

(B) The applicant is requesting more than the minimum amount of confidential data the applicant needs;

(C) The applicant is requesting other entities to be able to use, control, observe, transmit or store ~~control~~ confidential data who are not necessary for applicant's proposed use; or

(D) The data applicant will use, control, observe, transmit or store the confidential data outside of the United States of America;

(6) Regarding applications for the direct transmission of confidential data:

(A) The proposed use of the confidential data can be reasonably achieved by accessing confidential data through the enclave; or

(B) The data security for the confidential data does not meet the standards and requirements in section 97406; or

(7) The proposed use of program data is for determinations regarding individual patient care or treatment, for individual eligibility or coverage decisions, or similar purposes.

(c) Discretionary Reasons for Denial. The Department may deny a data application, in whole or in part, if the Department determines there is good cause to deny the application, including, but not limited to, the following:

(1) The applicant does not comply with this Article;

(2) The applicant is required to submit data to the program and is not in compliance with this chapter; or

(3) The Department determines that the public interest served by disclosing the data does not outweigh the public interest served by not disclosing the data.

Note: Authority cited: Section 127673, Health and Safety Code. Reference: Sections 127673.8, 127673.81, 127673.82, and 127673.83, Health and Safety Code.

§97390. Applications for Non-Confidential Program Data

(a) Data Application. To request program data that does not contain confidential data, an individual or organization must electronically submit an application with all of the following:

(1) Date of application.

(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) A detailed description of the requested data to allow the Department to determine whether the data exists, or whether it can be created.

(6) An explanation why the data applicant wants the data, including a description of the data use, the applicant's goals, and how the data will be used for purposes consistent with the program.

(7) How the data applicant wants to receive the data, either through the enclave or direct transmission.

(8) If accessed through the enclave, anticipated length of time the data applicant wants the data available.

(9) Project Title

(10~~9~~) Signature of the data applicant, if an individual, or the authorized representative, and the date of signature. This signature shall certify the information provided in the application.

Note: Authority cited: Section 127673, Health and Safety Code. Reference: Section 127673.81, Health and Safety Code.

§97392. Applications for Standardized Limited Datasets Through the Enclave

(a) Data Application. To request access to Standardized Limited ~~d~~Datasets through the enclave, an individual or organization must electronically submit an application with all of the following:

~~(1) Date of application.~~

(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 HCAI data 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 of the point of contact.

(7) Project Title

(8~~5~~) Identification of the specific Standardized Limited Dataset, a description of how the project meets the purposes specified by the Department for the Standardized Limited Dataset, and the time period of the requested data. ~~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~~6~~) A description of the research or analysis purpose for the data, the anticipated use of those data, and how the purpose is consistent with program goals. This includes a description of public data products that may be created with limited data 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~~7~~) Anticipated length of time the data applicant will need the confidential data in the enclave.

(12~~8~~) List of any data from outside the program which the data applicant wants to use or link with the confidential data.

(13~~9~~) List of all ~~contractors and~~ individuals, contractors and other third parties, who are anticipated to ~~observe, use, or control~~ use, control, observe, transmit or store confidential data and the physical location(s) from which they may work. This includes each ~~contractor's or~~ individual's, contractor's or other third parties', name, organization, phone number, business address, email address, title,~~position~~ 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 the contract(s) or agreement(s) between the collaborating entities.

(15~~10~~) 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.

(16~~11~~) 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.

(17~~12~~) 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.

(18) The applicant's data 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.

(19) 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 required access level and any additional software or tools required.

(2013) Signature of the data applicant(s), if an individual or individuals, or the authorized representative, and the date of signature. This signature shall certify the information provided in the application.

(b) Other Mandatory Reason 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 the proposed use of the requested confidential data is not for research or analysis purposes.

Note: Authority cited: Section 127673, Health and Safety Code. Reference: Sections 127673.81, 127673.82, and 127673.83, Health and Safety Code.

§97393. Applications for Custom Limited Datasets Through the Enclave

(a) Data Application. To request access to Custom Limited Data through the enclave, an individual or organization must electronically submit an application 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 HCAI data 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 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) A description of the research or analysis purpose for the data, the anticipated use of those data, and how the purpose is consistent with program goals. This includes a description of public data products that may be created with limited data 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) 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, title, phone number, business address, email address, 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 the contract(s) or agreement(s) between the collaborating entities.

(15) 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.

(16) 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.

(17) 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.

(18) The applicant's data 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.

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

(20) 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 required access level and any additional software or tools required.

(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 the information provided in the application.

(b) Other Mandatory Reason 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 the proposed use of the requested confidential data is not for research or analysis purposes.

Note: Authority cited: Section 127673, Health and Safety Code. Reference: Sections 127673.81, 127673.82, and 127673.83, Health and Safety Code.

§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 with all of the following:

~~(1) Date of application.~~

(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 HCAI data 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 of the point of contact.

(7) Project Title

(8~~5~~) 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~~6~~) A description of the research project, the anticipated use of the data, and how 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~~7~~) Anticipated length of time the data applicant will need the confidential data in the enclave.

(12~~8~~) List of any data from outside the program which the data applicant wants to use or link with the confidential data.

(13~~9~~) List of all ~~contractors and~~ individuals, contractors and other third parties, who are anticipated to ~~observe,~~ use, ~~or~~ control, observe, transmit or store confidential data and the physical location(s) from which they may work. This includes each ~~contractor's or~~ individual's, contractor's or other third parties'

name, organization, title, phone number, business address, email address, ~~position~~ 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 ~~third party~~contractor or other third party, a copy of any~~the~~ contract(s) or agreement(s) between the collaborating entities.

(15~~10~~) 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~~11~~) 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~~12~~) 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~~13~~) 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~~contractors~~.

(19) The applicant's data 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~~14~~) 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.

~~(15) 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, or the data applicant's plan to seek the Committee's approval during~~

~~the Department's review or after the Department conditionally approves the application pursuant to section 97410.~~

(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 required access level and any additional software or tools required.

(24~~16~~) Signature of the data applicant(s), if an individual or individual(s), or the authorized representative, and the date of signature. ~~=~~This signature shall certify the information provided in the application.

(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 Committee for the Protection of Human Subjects pursuant to subdivision (t) of Section 1798.24 of the Civil Code does not approve the research project~~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.

Note: Authority cited: Section 127673, Health and Safety Code. Reference: Sections 127673.81, 127673.82, and 127673.83, Health and Safety Code.

§97396. Applications for the Direct Transmission of Standardized Limited Datasets

(a) Data Application. To request direct transmission of a standardized limited dataset~~, either in whole or in part,~~ an individual or organization must electronically submit an application with all of the following:

~~(1) Date of application.~~

(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 HCAI data 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 of the point of contact.

(7) Project Title

(8~~5~~) Identification of the standardized limited dataset the data applicant wants, ~~including~~ 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~~, and a list of confidential data elements from the standardized limited dataset that the data applicant is not requesting, if any~~.

(9~~6~~) A description of the data use, and how the purpose is consistent with program goals.~~how the use is consistent with the purpose of the standardized limited dataset that the Department specified.~~ 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~~7~~) Explanation why the data applicant needs direct transmission of the confidential data instead of accessing the data through the enclave.

(12~~8~~) Anticipated length of time the confidential data will be needed to accomplish the use.

(13~~9~~) List of any data from outside the program which the data applicant wants to use or link with the confidential data.

(14~~10~~) List of all ~~contractors and~~ individuals, contractors and other third parties, who are anticipated to ~~observe, use, or control~~ use, control, observe, transmit or store confidential data and the physical location(s) from which they may work. This includes each ~~contractor's or~~ individual's, contractor's, or other third parties' name, organization, title, phone number, business address, and email address. ~~position~~

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~~11~~) 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~~12~~) 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~~13~~) 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~~14~~) 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~~15~~) Name, phone number, and email address of the individual who will be responsible for information security of the confidential data.

(21~~16~~) Signature of the data applicant(s), if an individual or individuals, or the authorized representative, and the date of signature. This signature shall certify the information provided in the application.

(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; or

(3) The Data Release Committee did not recommend project approval.

(4) Application includes request for identifiable provider information.

Note: Authority cited: Section 127673, Health and Safety Code. Reference: Sections 127673.81, 127673.82, and 127673.83, Health and Safety Code.

§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 with all of the following:

~~(1) Date of application.~~

(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 HCAI data 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 of the point of contact.

(7~~5~~) Whether the applicant or the affiliated organization submits data to the program.

(8) Project Title

(9~~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 data applicant needs each confidential data element.

(10~~7~~) 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~~8~~) Explanation of why the data applicant needs direct transmission of the confidential data instead of accessing the data through the enclave.

(13~~9~~) Anticipated length of time the confidential data will be needed to accomplish the project.

(14~~10~~) 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 the data.

(15~~11~~) List of all ~~contractors and~~ individuals, contractors and other third parties, who are anticipated to ~~observe, use, or control~~ use, control, observe, transmit or store confidential data and the physical location(s) from which they may work. This includes each ~~contractor's or~~ individual's contractor's or other third parties' name, organization, title, phone number, business address, email address, ~~position~~ 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~~12~~) 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~~13~~) 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~~14~~) 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~~15~~) 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~~16~~) Name, phone number, and email address of the individual who will be responsible for information security of the confidential data.

(23~~17~~) A statement by the applicant agreeing to make the research from the research project available to the Department.

(24~~18~~) A copy of the applicant's draft or submitted application to the Committee for the Protection of Human Subjects. ~~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, or the data applicant's plan to seek the Committee's approval during the Department's review or after the Department conditionally approves the application pursuant to section 97410.~~

(25~~19~~) Signature of the data applicant(s), and the date of signature. ~~-~~This signature shall certify the information provided in the application.

(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 Committee for the Protection of Human Subjects pursuant to subdivision (t) of Section 1798.24 of the Civil Code did not approve the research project or 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~~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.

Note: Authority cited: Section 127673, Health and Safety Code. Reference: Sections 127673.81, 127673.82, and 127673.83, Health and Safety Code.

§97400. State Agency Applications for Confidential Data

(a) Data Application. For state agencies requesting confidential data, a state agency must electronically submit an application with all of the following:

~~(1) Date of application.~~

(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~~5~~) 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.

(7~~6~~) 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 applicant is requesting access to Medi-Cal data, how the use of the data will contribute to the project.

(9~~7~~) How the state agency wants the data, such as through the enclave or by direct transmission. If by direct transmission, an explanation why the data applicant needs direct transmission of the confidential data instead of accessing the data through the enclave.

(10~~8~~) Anticipated length of time the confidential data will be needed to accomplish the project.

(11~~9~~) List of any data from outside the program which the state agency wants to use or link with the confidential data.

(12~~10~~) List of all ~~contractors and~~ individuals, contractors and other third parties, who are anticipated to ~~observe, use, or control~~ use, control, observe, transmit or store confidential data and the physical location(s) from which they may work. This includes each ~~contractor's and~~ individual's contractor's or other third parties'

name, organization, title, phone number, business address, email address, ~~position~~ 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 applicant is working with a contractor or other third party, a copy of the contract(s) or agreement(s) between the collaborating entities.

(14~~11~~) 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.

(15~~12~~) 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.

(16~~13~~) 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, ~~and~~ background screening for individuals who will access the data, and a description of how the data security standards and requirements in section 97406(b) will be met. This includes the specific data access method for any contractors or third parties.; or

(B) If requesting direct transmission of confidential data, the data 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 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 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 required access level and any additional software or tools required.

(18~~714~~) Signature of the authorized representative of the state agency, and the date of signature. This signature shall certify the information provided in the application.

(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 applicant to perform its constitutional or statutory duties; or

(2) The applicant's proposed use of the confidential data is incompatible with a purpose for which the data was collected.

Note: Authority cited: Section 127673, Health and Safety Code. Reference: Sections 127673.81, 127673.82, and 127673.83, Health and Safety Code; and Section 1798.24, Civil Code.

§97402. Data Release Committee

(a) To access confidential data under Sections 97394, 97396, or 97398, it is required that the Data Release Committee recommend approval of the data applicant's project.

(b) Once the data applicant completely submits an application under Sections 97394, 97396, or 97398, the Department shall send the Data Release Committee a copy of the application for the Committee to make its recommendation.

(c) The Data Release Committee shall consider the applicant's project during one or more of its public meetings and may require the attendance of the applicant at a meeting to present or respond to questions and issues. After the meeting, the Data Release Committee shall issue a written recommendation regarding the applicant's project.

Note: Authority cited: Section 127673, Health and Safety Code. Reference: Sections 127673.83, and 127673.84, Health and Safety Code.

§97404. Committee for the Protection of Human Subjects

(a) To access confidential data under Sections 97394 or 97398, it is required that the Committee for the Protection of Human Subjects approve the data applicant's project pursuant to subdivision (t) of Section 1798.24 of the Civil Code.

(b) The applicant may seek the approval of the Committee for the Protection of Human Subjects before or concurrently with its data application to the Department~~, or may wait after the Department conditionally approves the application pursuant to section 97410 to seek the Committee's approval.~~

Note: Authority cited: Section 127673, Health and Safety Code. Reference: Sections 127673.83, Health and Safety Code.

§97406. Data Security Standards for ~~Direct Transmission of~~ Standardized Limited Datasets and Other Confidential Data

(a) The following definitions apply to this section:

(1) "NIST" is the National Institute of Standards and Technology, an agency of the United States of America.
(2) "FIPS 140 Validation" means current validation by the NIST's Cryptographic Module Validation Program that a module conforms to the standards of the currently applicable Federal Information Processing Standards Publication 140.
(3) "FIPS 200" means the Federal Information Processing Standards Publication 200, "Minimum Security Requirements for Federal Information and Information Systems," dated March 2006, which is hereby incorporated by reference.
(4) "Information system" means an applicant's discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of confidential data.
(5) "NIST 800-53" means the NIST Special Publication 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations," dated September 2020; and NIST Special Publication 800-53B, "Control Baselines for Information Systems and Organizations," dated October 2020, both of which are hereby incorporated by reference.
(6) "NIST 800-88" means Section 5 and Appendix A of the NIST Special Publication 800-88, Revision 1, "Guidelines for Media Sanitization," dated December 2014, which are hereby incorporated by reference.

(b) All HPD applicants must meet the following requirements:

(1) Anyone accessing HPD data shall receive training on information privacy and data security no less than once per year for the duration of their access to HPD data.
(2) All software, information systems, computers, and other devices that are used to access HPD data, including through the Enclave, shall have security patches applied in a reasonable time.
(3) Passwords to access HPD data shall, at a minimum, have 16 characters with at least one capital letter, one small letter, one number, and one special character.
(4) All information systems, computers, and other devices that are used to access HPD data, including through the Enclave, shall have active antivirus controls. Applicants must provide the security antivirus controls in place by product name and current version.

~~(b)~~ (c) For direct transmission of confidential data under Sections 97396, 97398, or 97400, a data applicant must provide a level of data security for confidential data that is

not less than the level required by FIPS 200 and NIST 800-53 for information that is categorized as moderate-impact for the security objective of confidentiality.

~~(c)~~ (d) Notwithstanding the above, applicants applying for direct transmission of confidential data under Sections 97396, 97398 or 97400 shall comply with the following security requirements:

(1) Applicants shall conduct a thorough background check of each individual who will observe, use, or control confidential data on their behalf before the individual has the ability to observe, use, or control the data. This background check shall, at the least, include the individual's history of data breaches, and criminal convictions or substantiated violations of law regarding fraud, theft, data breach, data misuse or related offenses. Based on the thorough background check, applicants shall evaluate whether the individual presents an unreasonable risk of causing a data breach, stealing confidential data, or misusing confidential data and prohibit those who present such a risk from having the ability to observe, use, or control the data. Applicants shall document each background check and evaluation and retain these records for a period of three (3) years after the applicant stops using the confidential data.

(2) All computers containing confidential data shall have full disk encryption using modules with FIPS 140 validation.

~~(1)~~ (3) All removable media devices containing confidential data shall be encrypted with software that has FIPS 140 validation.

~~(2)~~ (4) If the Department approves transmittal of confidential data outside of the applicant, the following is required:

(A) all electronic transmissions of confidential data outside the information system shall be encrypted using software that has FIPS 140 validation;

(B) all mailings of unencrypted confidential data, including hardcopies, shall be sealed, and secured from view by unauthorized individuals and shall be mailed using a tracked mailing method, which includes verification of delivery and receipt.

~~(3)~~ (5) Unencrypted confidential data, including hard copies, shall be stored, and used within applicant's work offices, and when unattended, shall be stored in secured areas with controlled access procedures, where it is not viewable from the outside, and is under 24-hour guard or monitored alarm.

~~(4)~~ (6) Direct personal identifiers listed in Section 164.514(e) of Title 45 of the Code of Federal Regulations shall be stored separately from other confidential data.

~~(5)~~ (7) Regarding media sanitization, hard copy and digital media with confidential data shall be disposed of as described in NIST 800-88.

~~(6) All software, information systems, computers, and other devices that process, store, or use confidential data shall have security patches applied in a reasonable time.~~

~~(7) Passwords to access confidential data shall, at a minimum, have 16 characters with at least one capital letter, one small letter, one number, and one special character.~~

~~(8)~~ (8) The applicant must use signature based and non-signature based malicious code protection mechanisms at system entry and exit points.

(c) If applicants cannot meet a security requirement in subsection, they may request exceptions to the requirement in their data application to the Department. The Department shall only grant an exception if it determines that the applicant has adequate alternatives.

Note: Authority cited: Section 127673, Health and Safety Code. Reference: Sections 127673.5, 127673.6, 127673.81, 127673.82, and 127673.83, Health and Safety Code.

§97408. Special Requirements for Medi-Cal Information

(a) An applicant seeking confidential data that includes Medi-Cal information from the California Department of Health Care Services must provide the following additional information in its data application:

(1) Specify how the proposed project will benefit the administration of the Medi-Cal program;

(2) The funding sources for applicant's project; and

(3) Whether the project will assist in the development of a commercial product.

(b) An application for Medi-Cal information is subject to review by the California Department of Health Care Services. Once the applicant completely submits its application, the Department shall send the Department of Health Care Services a copy of the application for review.

(c) A request for Medi-Cal information shall be denied if the Department of Health Care Services denies the applicant's request for Medi-Cal information.

Note: Authority cited: Section 127673, Health and Safety Code. Reference: Section 127673.82, Health and Safety Code; 42 U.S.C. section 1396a; and Section 14100.2, Welfare and Institutions Code.

§97410. Decisions on Data Applications

(a) Timelines for Decisions.

(1) The Department shall notify applicants in writing of its decision on the data application within 120 days of the complete submission of the data application unless one or more of the following occur:

(A) A longer period is agreed to by the applicant; or

(B) For data applications in which a Data Release Committee recommendation is required or if the Department requests input from the Committee~~, within 15 days of receiving input or the recommendation from the Committee~~; or

(C) The data request includes data subject to review by the Department of Health Care Services under Section 97408; or

(D) The data request includes confidential data, which requires approval from the Committee for the Protection of Human Subjects; or

(E) If the Department has good cause to extend time.

(2) If there is an extension of time under this section, the Department shall notify the applicant in writing of the extension, including the reason for the extension and the anticipated length of extension. The Department shall send this notice to applicant at least 10 days before the Department is required to issue a decision notice.

(b) Decision Notice.

(1) If the application is denied, in whole or in part, the Department shall state in the notice the scope of denial and the reasons for denial.

(2) If the application is approved, in whole or in part:

(A) The Department shall state in the notice the scope of the approval, the ~~fee~~ price for the data as set by the Department, and how the data will be provided to the applicant; and

(B) If a data use agreement is required pursuant to section 97412, the Department shall provide the required data use agreements with the decision notice, and the reason why data use agreements are required.

~~(c) Conditional Decision Notices. For data applications which require the approval of the Committee for the Protection of Human Subjects, the Department may issue a notice of conditional approval before the Committee makes its decision.~~

~~(1) The applicant shall provide the Department with the Committee's decision within 10 days of receiving the decision.~~

~~(2) Within 30 days of receiving the Committee's decision from the data applicant, the Department shall issue a final decision notice to the applicant. The Department's final decision may be different from its notice of conditional approval.~~

Note: Authority cited: Section 127673, Health and Safety Code. Reference: Sections 127673.82, and 127673.83, Health and Safety Code.

§97412. Data Use Agreements ~~for Confidential Data~~

(a) Required Data Use Agreements.

(1) Prior to receiving confidential data pursuant to an approved data application:

(A) Each approved applicant shall execute a data use agreement.

(B) Each person ~~individual~~ who will observe, use, or control confidential data under an approved application shall execute a data use agreement.

(2) For non-confidential program data, the Department may, for good cause, require an approved applicant or the persons ~~individuals~~ who will observe, use, or control program data to execute data use agreements.

(b) Contents for Confidential Data Use Agreements ~~for Applicants and Individuals~~. A data use agreement between the Department and the applicant or persons ~~individuals~~ approved for confidential data under this Article shall have, at least, the following:

(1) The applicant or person ~~individual~~ shall only observe, use, control, or store confidential data in the United States of America.

(2) The data use agreement shall be governed, and construed in accordance with, the laws of the State of California and all litigation that may arise as a result of the agreement shall be litigated in the Superior Court of California, County of Sacramento.

Note: Authority cited: Section 127673, Health and Safety Code. Reference: Sections 127673.82, and 127673.83, Health and Safety Code.

§97414. ~~Fee~~ Price Reduction

(a) For specific data applications, the Department may reduce program data ~~fees~~ prices on the Department's ~~fee~~ price schedule if it determines there is good cause for reduction, supported by documentation. Good cause includes, but is not limited to:

(1) the financial hardship of data applicants, such as students with needs-based financial aid working toward completion of required academic milestones, or government or nonprofit organizations whose funding sources for their projects do not cover data ~~fees~~ prices; or

(2) whether reduction will encourage the use of program data in high priority areas, or will lead to innovations that will benefit the public at large.

(b) Data applicants may request a reduction by submitting with their data application their justification for reduction with supporting documentation. During its review, the Department may seek more information from data applicants about their reduction requests.

(c) The Department shall notify the data applicant of its determination in the decision notice required under Section 97410 with its reasons for denial or approval.

(d) Price reductions will be considered on a per project basis.

(e) Price reduction requests will be considered in the order received until available funds for price reductions are exhausted or price reductions are no longer compatible with program sustainability.

(f) Partial price reductions will be considered. Full price reductions may be considered for any project if supported by sufficient justification and documentation.

Note: Authority cited: Section 127673, Health and Safety Code. Reference: Sections 127673.82, and 127674, Health and Safety Code.

§97416. Restrictions for Public Data Products

(a) Data users shall not include PII or record-level information about patients or individual consumers in their public data products. Data users shall only include aggregated and deidentified data about patients or individual consumers in their public data products.

(1) To deidentify aggregated data, data users must use the methodology stated in Sections 4 (regarding Steps 1 to 4), 4.1 to 4.4, 5.1 to 5.4, 6.1, 6.2, 6.4, and 9 of the California Health and Human Services Agency's "Data De-Identification Guidelines (DDG)," dated September 23, 2016. Data users shall use the "Publication Scoring Criteria" stated in Section 4.3 of the DDG as their method to assess potential risk. These sections are hereby incorporated by reference.

(b) Data users shall submit draft public data products with any information about patients or individual consumers to the Department. The Department shall review these draft public data reports for compliance with subsection (a).

(1) Data users shall submit with their draft public data products documentation regarding how they aggregated and deidentified the PII or record-level information about patients or individual consumers.
(2) Data user shall not release public data products unless the Department approved the release of the public data product in writing. If the Department does not approve a draft public data product, it shall notify the data user in writing of its decision and the reasons for its decision.

(c) Data users shall not include PII or record-level data regarding individuals who are not patients or individual consumers in their public data products if ~~such disclosure infringes on an individual's privacy or safety.~~ the Department determines that the disclosure would be a mandatory reason for denial under section 97388(b) or if the Department determines that there is good cause to prevent the disclosure.

(1) Data Users shall notify the Department if their draft public data products include PII or record-level information regarding individuals who are not patients or individual consumers. This notice shall describe the PII or record-level information.
(2) The Department may require its review and approval of these draft public data products before release for compliance with this subsection. Data users shall not release the public data product before the Department notifies the data user whether review is required.
(3) If review is required, the following shall apply:
    (A) Data users shall not release draft public data products under review unless the Department approved the release of the public data product in writing.

(B) If the Department does not approve the draft public data product, it shall notify the data user in writing of its decision and the reasons for its decision. The Department may require information about individuals to be aggregated or deidentified pursuant to subsection (a) before release.

Note: Authority cited: Section 127673, Health and Safety Code. Reference: Sections 127673.5, 127673.81, and 127673.82, Health and Safety Code.