INITIAL STATEMENT OF REASONS

HEALTH CARE PAYMENTS DATA PROGRAM DATA USE, ACCESS, AND RELEASE

CALIFORNIA CODE OF REGULATIONS
TITLE 22, DIVISION 7, CHAPTER 11, ARTICLE 8
SECTIONS 97380 TO 97416

[05/22/2023]

Pursuant to California Government Code section 11346.2(b), the California Department of Health Care Access and Information (HCAI) hereby presents its initial statement of reasons for its proposed regulations regarding the Health Care Payments Data Program's (HPD) data use, access, and release program.

I. BACKGROUND INFORMATION

The Department of Health Care Access and Information (HCAI) is required to establish the Health Care Payments Data Program (HPD) by California Health and Safety Code (HSC) sections 127671 to 127674.1.[1] The HPD is to collect health care data from health care plans, health insurers, government agencies, and others and to use this data to provide greater transparency regarding health care costs, utilization, quality, and equity and to improve health care in California.[2]

As required by statute,[3] HCAI already promulgated emergency regulations for the collection of HPD data on December 20, 2021. HCAI started collecting routine HPD data in November 2022.[4]

II. THE PROBLEM TO BE ADDRESSED AND PURPOSE OF THESE REGULATIONS

[1] Enacted by Assembly Bill No. 80 (2019-2020 Reg. Sess.).
[2] *See* HSC section 127671 [regarding the HPD and its purposes].
[3] HSC section 127673(e).
[4] Cal. Code Regs, title 22, section 97352(a).

A statutory purpose of the HPD is to release HPD data to members of the public and other state agencies so they can use the data to improve health care in California.[5] HPD statute states that the HPD should:

> "encourage state agencies, researchers, health care service plans, health insurers, providers, suppliers, and other stakeholders to use [HPD] data to develop innovative approaches, services, and programs that may have the potential to deliver health care that is both cost effective and responsive to the needs of enrollees, including recognizing the diversity of California and the impact of social determinants of health."[6]

However, the HPD will collect a large volume of private personal data about individual Californians including Social Security Numbers, dates of birth, medical diagnoses, prescribed drugs, and other medical information.[7] Uncontrolled release of this information would be incredibly damaging to individuals and would result in massive privacy violations. For this reason, HPD statute makes clear that although HPD data should be released to data users, HCAI must "preserv[e] consumer privacy"[8] and that HCAI must ensure "that the privacy, security, and confidentiality of consumers' individually identifiable health information is protected."[9]

Furthermore, HPD statute exempts all HPD data, including non-personal data, from the disclosure requirements of the California Public Records Act (CPRA).[10] Based on this, the public cannot receive HPD data unless HCAI creates a program to provide such data. These regulations create this program to access HPD data.

Based on the above, HPD statute requires HCAI to establish a "data use, access, and release program" to provide HPD data to outside entities while protecting privacy.[11] HPD statute then states how private HPD data can be made available to members of the public and other state agencies[12] and provides minimum "privacy protection standards" which can be supplemented through these regulations.[13] For the most private data, HPD statute also requires approvals from one or two state committees.[14]

These regulations are to create the HPD's Data Use, Access, and Release Program, and implement the statutory requirements discussed above. HCAI attempts to balance

---

[5] HSC section 127673.82(c).
[6] HSC section 127671(d).
[7] *See* HSC section 127673(b) [regarding what data is to be collected by HPD].
[8] HSC section 127671(b) [regarding intent of the HPD].
[9] HSC section 127673.5(a)(2).
[10] HSC section 127673.81(c)(1). The California Public Records Act is codified in Cal. Gov. Code sections 7920.000, *et seq*.
[11] HSC section 127673.82(b).
[12] *See* HSC 127673.83.
[13] *See* HSC section 127673.83.
[14] HSC section 127673.83(b)(2) and (c).

data access and data protection in these regulations, although HCAI will generally favor protection over release to prevent harm to individual Californians. In these regulations, HCAI defines what HPD data is protected and how members of the public and other state agencies can receive HPD data, including confidential HPD data. These proposed regulations will provide access but protect privacy primarily by screening data applicants through a comprehensive data application process and restrictions on how HPD data can be used and publicized.

Other than consumer privacy, HCAI also considered other issues in preparing these proposed regulations. Some have noted that release of health care pricing information, such as negotiated rates between health care providers and payers, may have anticompetitive effects that harm consumers.[15] However, there may be benefits from releasing this information. Others have raised concerns about the safety and privacy of individual health care providers, especially of those who provide sensitive services. As specific requests will be for many different purposes and from different types of requesters, HCAI will address these issues by reviewing each request, requester, and a requester's data products on a case-by-case basis.[16] Also, HCAI can address these issues, based on the specific request and requester, through the statutorily-required data use agreements for HPD data users.[17]

HCAI used the California Department of Justice's data access and use regulations regarding its Controlled Substance Utilization Review and Evaluation System[18] (hereinafter the "CURES regulations") as a template for these regulations because the Department of Justice is required to allow research and analysis of the CURES database but must also protect the highly sensitive and private medical information in that database.[19]

III. BENEFITS OF THIS REGULATORY ACTION

The hope for these regulations that establish the HPD's Data Use, Access and Release Program is that outside entities will be able to receive and use HPD data to supplement and add to the work being done by HCAI to analyze HPD data and thus, maximize the

[15] *See* Katherine L. Gudiksen, Samuel M. Chang, and Jaime S. King, *The Secret of Health Care Prices: Why Transparency is in the Public Interest*, July 2019, page 11, available at https://www.chcf.org/publication/secret-health-care-prices/ (last accessed 3/16/2023) [discussing potential anticompetitive and competitive effects from pricing information disclosures].
[16] *See* proposed regulations, Cal. Code Regs., title 22, sections 97388 [regarding mandatory and discretionary reasons to deny HPD data request]; 97390 to 97400 [application requirements for HPD data requests]; and 97416 [regarding requirements for public data products].
[17] HSC section 127673.82(a) [requiring data use agreements for HPD data users]; *see* proposed regulations, Cal. Code Regs., title 22, section 97412 [regarding HPD data use agreements].
[18] For the CURES regulations, Cal. Code Regs, title 11, sections 820, *et seq*.
[19] HSC sections 11165(a) [CURES, in part, "for statistical analysis, education, and research…"] and 11165(c) [Statutory requirement "to safeguard the privacy and confidentiality of patients].

usefulness of HPD data and bring more benefits to California. Through the analysis and research of HPD data, it is hoped health care entities will be able to innovate their services and programs to provide more cost effective and responsive health care to Californians. Also, it is hoped that the disclosure of HPD data to analysts and researchers will reveal and publicize gaps in health care and will help address inequities in health care access throughout the state. Data disclosure will also increase openness and transparency in businesses and governmental agencies involved in health care.

These regulations, while potentially providing access to a vast sum of data as required by statute, will also diligently protect sensitive and private HPD data so that it will not be improperly used or disclosed to harm individual Californians.

IV. SPECIFIC PURPOSE AND NECESSITY OF EACH PROPOSED REGULATION

The following will go through each regulation and present the purpose of each regulation and that it is reasonably necessary to carry out the purposes of the HPD.

1. California Code of Regulations (CCR), title 22, section 97380, "Additional Definitions for this Article"

HCAI proposes this regulation for the purpose of providing definitions for several terms used in later proposed regulations in this Article for the HPD Data Use, Access, and Release Program. The definitions are needed to ensure that the regulations that follow meet the clarity requirement and to provide the specificity necessary for compliance with the regulations.

Article 1 of this chapter (Cal. Code Regs., title 22, section 97300) has general regulatory definitions for all of the HPD regulations. HCAI created a separate definition regulation for Article 8 because Article 8 has many definitions that just apply to the HPD Data Use, Access, and Release Program, and because Section 97300 is going through a separate rulemaking process.[20]

Specific explanations for each definition are below:

a. Terms in Section 97380, subdivisions (a) "Aggregated data":

HPD statute requires that HCAI develop "policies and procedures" for the disclosure of aggregated and deidentified individual consumer and patient data "in a publicly available analysis, data product, or research"[21] and regarding "data aggregation and the

[20] *See* HSC section 127673(e) and (f) [statute required the initial HPD regulations to be emergency regulations and will repealed by operation of law on December 20, 2023 unless a Certificate of Compliance is filed].
[21] HSC section 127673.81(c)(2).

protection of individual confidentiality, privacy, and security for individual consumers and patients."[22] As discussed later, Section 97416 is intended for these purposes.

Subsection (a) defines what "aggregated data" means so it is very clear what the Department means by this term to achieve the statutory purposes discussed above.

The first part of the definition is that "aggregated" data does not have any record-level or an individual consumer/patient's data. This is from the dictionary definition that "aggregate" means "formed by the collection of units or particles into a body, mass, or amount."[23] The second part of the definition is that "aggregated" data only has collective data relating to a group or category" is from the California Health and Human Services Agency's "Data De-Identification Guidelines (DDG)," dated September 23, 2016, page 6.[24] HCAI believes this definition clearly and definitively defines "aggregated data" as meant by HPD statute to protect patient and consumer privacy.

b. Term in Section 97380, subdivisions (b) "Authorized representative":

For data applicants who are not individuals, a single point of contact is needed from the data applicant, so HCAI knows who to contact regarding a data request or HPD data. This individual must be authorized to act on behalf of the organizational data applicant and must have responsibility over the HPD data for the applicant so HCAI knows that the individual can meaningfully respond to questions or issues about HPD data.

As this individual is referenced many times in these regulations, HCAI seeks to have a simple term, "authorized representative," for this individual to increase clarity and so that HCAI does not have to repeatedly explain this term in multiple places.

c. Term in Section 97380, subdivisions (c) "Confidential data":

HPD statute is concerned with protecting certain data the HPD will collect from public disclosure for privacy reasons. This protected data is identifiable or record-level data about consumers or patients pursuant to several HPD statutes.[25] As discussed earlier,

[22] HSC section 127673.5(b)
[23] Merriam-Webster Dictionary, Definition of "aggregate" adjective, https://www.merriam-webster.com/dictionary/aggregated (last accessed 11/10/2022).
[24] The California Health and Human Services Agency's "Data De-Identification Guidelines (DDG)," dated September 23, 2016, is available here https://chhsdata.github.io/dataplaybook/documents/CHHS-DDG-V1.0-092316.pdf (last accessed 11/10/2022).
[25] HSC sections 127673.5(a)(2) [HCAI "shall ensure that the privacy, security, and confidentiality of consumers' individually identifiable health information is protected"]; and 127673.81(a) ["All personal consumer information obtained or maintained by the [HPD] shall be confidential" and "Only deidentified aggregate patient or other consumer data shall be included in a publicly available analysis, data product, or research."]

these regulations are about protecting this data from public disclosure when provided to those outside of HCAI.[26]

As this term is used throughout these regulations, HCAI proposes to have a single simple term for this protected data and defines it here as "confidential data" for clarity and so that this does not have to be repeatedly explained.

d. Terms in Section 97380, subdivisions (d) "Data Applicant" or "Applicant:

Several subsequent regulations use the term "data applicant" or "applicant." HCAI introduces and defines this term here to make clear what this means—an individual or organization that submits an application for HPD data under these regulations.

e. Terms in Section 97380, subdivisions (e) "Data Product" and (n) "Public Data Products":

HPD statute only allows deidentified aggregated patient or consumer data to "be included in a publicly available analysis, data product, or research."[27] HCAI is required to "develop policies and procedures for the disclosure" of this type of information.[28]

HCAI proposes these definitions to have simple terms to refer to information that is derived from program data and for such information that is to be publicly released because there are multiple regulatory requirements for these "data products." This is for clarity and so that these terms do not have to be repeatedly explained.

f. Term in Section 97380, subdivisions (f) "Data Release Committee":

HPD statute creates the HPD "data release committee" to advise HCAI and to review and approve certain HPD data requests.[29] As this committee is involved in the HPD data release process, several subsequent regulations refer to this committee. For clarity and to not have to repeatedly define the committee, HCAI defines a term for this committee here.

g. Term in Section 97380, subdivisions (g) "Data User":

[26] *See* HSC sections 127673.5(b) [HCAI "shall develop policies" regarding protection of individual data for "individual consumers and patients"]; and 127673.81(c)(2) [HCAI "shall develop policies and procedures for the disclosure of" deidentified aggregate patient or other consumer data].
[27] HSC section 127673.81(a)(2).
[28] HSC section 127673.81(c)(2).
[29] HSC section 127673.84.

HCAI created a term for those entities that are approved to receive HPD data, i.e., "data user," to distinguish from "data applicants" as subsequent regulations limited how HPD data is used once an individual or organization receives HPD data. This makes the regulations clearer and prevents the need to explain this term repeatedly.

h. Term in Section 97380, subdivisions (h) "Direct Transmission":

HPD statute allows for two ways to release of confidential HPD data: (1) through the secure online data access environment or "Enclave" that HCAI is to develop, and (2) transmittal of data to entities.[30] HPD statute has more stringent requirements for confidential data transmittal than through the Enclave. Because of the different statutory requirements and because transmittal of data has more data security risks, multiple regulations reference these two methods separately.

For clarity, HCAI defines the term "direct transmission" as its way of easily noting the transmittal method discussed above and to be very clear what this means—i.e., sending copies of data outside of the "Enclave." This is in contrast to accessing data through the "Enclave" (a term defined later).

i. Term in Section 97380, subdivisions (i) "Enclave":

HPD statute requires HCAI to establish a "secure research environment" for data users to virtually access confidential HPD data.[31] For clarity and ease of use, HCAI proposes to use the simpler term, "Enclave," for the secure research environment. The term "Enclave" is also in common use to refer to secure research environments like the one HCAI is to establish for HPD.[32]

j. Term in Section 97380, subdivisions (j) "Limited Data":

HPD statute allows for the release of confidential HPD data that does not include "direct personal identifiers listed in Section 164.514(e) of Title 45 of the Code of Federal Regulations."[33] For this reason, subsequent regulations refer to this type of data several times regarding how entities can access this type of data. To have a simpler term for this data to use in regulations, HCAI proposes to use the term, "limited data," for this type of data. HCAI also wishes to use this term because this type of data is

[30] HSC section 127673.83 [discussing access to HPD data through the Enclave and transmittal of HPD data].
[31] HSC section 127673.82(d).
[32] *See, for example*, the University of Chicago, *Secure Data Enclave*, https://securedata.uchicago.edu/ (last accessed 10/25/2022); and the University of Michigan, Inter-university Consortium for Political and Social Research, *What is the Virtual Data Enclave (VDE)?*, https://www.icpsr.umich.edu/web/DSDR/cms/2014 (last accessed 10/25/2022).
[33] HSC section 127673.83(b)(1) and (c)(1).

commonly referred to as “limited data” in health care and would be understandable to those familiar with health care data.[34]

For clarity, the definition of “limited data” notes that it is a subset of “confidential data” (as discussed above) and includes “standardized limited datasets” (discussed later).

k. Term in Section 97380, subdivisions (k) “Personally Identifiable Information”:

HPD statute specifically protects “personally identifiable information” of patients and other consumers.[35] HCAI defines this statutory term and includes it in its definition of the term “confidential data” so that there is clear understanding what HPD data is subject to heightened protection and cannot be publicly released.

The proposed definition of “personally identifiable information” is substantially the same as the definition used by the federal government.[36] It was slightly modified to include “reasonably” which is from the definition of “individually identifiable health information” from the federal Health Information Portability and Accountability Act (HIPAA).[37]

Based on its use by the federal government, HCAI believes this definition is the common understanding of this term and adequately captures the type of information about consumers and patients that HPD statute intends to be protected from public disclosure to preserve an individual’s privacy.

l. Term in Section 97380, subdivisions (l) “Program Data”:

HPD statutes refer to HPD “program data” and that this “program data” is exempt from the CPRA and shall not be made available except under the HPD statutes.[38] HCAI uses and defines this term here to have a simple clear term to describe the data that is subject to these regulations.

---

[34] *See* Code Fed. Regs., title 45, section 164.514(e) [part of the Health Insurance Portability and Accountability Act (HIPAA), and referring to this data as “limited data sets”]; and HSC 127673.83(c)(1) [referring this data as “limited datasets”].

[35] HSC sections 127673(b)(3) [“personally identifiable information shall be subject to the privacy protections of this chapter and shall not be publicly available, except as specified in this chapter”]; 127673.5(a)(2) [HCAI “shall ensure that the hall ensure that the privacy, security, and confidentiality of consumers’ individually identifiable health information is protected….]; 127673.8(d) [public HPD materials “shall protect patient and consumer privacy]; and 127673.81(a) [“all personal consumer information obtained or maintained by the program shall be confidential”].

[36] *See* 2 C.F.R. section 200.1 [defining “personally identifiable information”]; the Federal Office of Management and Budget Circular No. A-130, “Managing Information as a Strategic Resource (revised July 2016); and NIST Special Publication 800-37, Revision 2 (December 2018).

[37] 45 C.F.R. section 160.103 [defining “individually identifiable information” for purposes of HIPAA].

[38] HSC section 127673.81(c)(1).

HCAI defines this term to mean all "information created, obtained, or maintained" by the HPD. This definition is from HPD statute which discusses "program data" that is "obtained or maintained" by the HPD.[39] HCAI also included "created" for any data products it may develop from HPD data to ensure the definition covers data that may not have been obtained or maintained.

m. Term in Section 97380, subdivisions (m) "Program Goals":

HPD statutes refer to HPD "program goals" several times and some requirements for data release require that the proposed use be at least consistent with "program goals."[40] HCAI defines "program goals" here so that the public and requesters have a clear understanding of what this term means in these proposed regulations. The goals of the HPD are stated in HPD statute and this definition references those HPD statutes.

n. Term in Section 97380, subdivisions (o) "Record-level":

HPD statute prohibits record-level information about patients and other consumers from being released publicly.[41] HCAI defines "record-level" here and includes it in its definition of the term "confidential data" so that there is clear understanding of what HPD data is subject to heightened protection and cannot be publicly released.

o. Term in Section 97380, subdivisions (p) "Research":

This term, "research," and the definition of this term is taken directly from statute, HSC section 127671(f)(6). It is included in this definitions section for clarity because many HPD data release regulations reference "research," such as sections 97380(r), 97392, 97394, and 97398.

p. Term in Section 97380, subdivisions (q) "Research Identifiable Data":

HPD statute allows for the release of confidential HPD data that includes the "direct personal identifiers listed in Section 164.514(e) of Title 45 of the Code of Federal Regulations" but only for research.[42] For this reason, subsequent regulations refer to this type of data several times regarding how entities can access this type of data. For clarity, the definition of "research identifiable data" notes that it is a subset of "confidential data" as discussed above.

[39] HSC section 127673.81(a)(1).
[40] HSC sections 127673.83(b)(1) and (2).
[41] HSC sections 127673.81(a)(2) [stating that "only deidentified aggregate patient or other consumer data shall be" publicly available]; and 127673.82(a) [HPD to make sure "that only aggregated, deidentified information is publicly accessible"].
[42] HSC section 127673.83(b)(2) and (c)(2).

To have a simpler term for this data to use in regulations, HCAI proposes to use the term, "research identifiable data," for this type of data which precisely describes this data. HCAI also wishes to use this specific term because the federal government uses the same term for the same type of data—i.e., data with the most direct identifiers which is only for research purposes.[43] By using this term, HCAI believes this would be easily understood by those are already familiar with health care data.

q. Term in Section 97380, subdivisions (r) "Researcher":

HPD statute limits one type of data request, the transmittal of confidential HPD data pursuant to section 97398, to "researchers" (as noted in proposed section 97382).[44] HCAI defines "researcher" here so that there is clear understanding regarding who HCAI considers to be researchers.

The proposed definition of "researcher" is adapted from the definition in the CURES regulations.[45] HCAI broadened the CURES definition more to allow those with degrees less than a master's degree to be considered "researchers" to allow students in postgraduate studies to be able to apply for the data. As seemingly intended by HPD statute in limiting certain data requests to "researchers," HCAI believes this definition adequately restricts the potential transmittal of confidential HPD data to professionals who have an adequate amount of experience and education in handling and maintaining confidential information.

r. Term in Section 97380, subdivisions (s) "Standardized Limited Datasets":

HPD statute allows for the release of confidential HPD data in the form of "standardized limited datasets."[46] This is a statutory term, and the definition is taken directly from statute, HSC section 127673.83(c)(1), except for the addition that the data sets are created with "confidential data," as discussed above. This is included in this definitions section for clarity.

2. CCR, title 22, section 97382, "Eligibility for Program Data"

[43] *See* Lori Siedelman, *Differences between RIF, LDS, and PUF Data Files*, Aug. 10, 2016, https://www.hhs.gov/guidance/document/differences-between-rif-lds-and-puf-data-files (last accessed 10/20/2022); Centers for Medicare & Medicaid Services, *Identifiable Data Files*, Dec. 1, 2021, https://www.cms.gov/Research-Statistics-Data-and-Systems/Files-for-Order/IdentifiableDataFiles (last accessed 10/20/2022); and Erin Mann, *Introduction to Research (RIF) Data,* Apr. 25, 2013, http://resdac.umn.edu/sites/resdac.umn.edu/files/Introduction%20to%20Research%20Identifiable%20Data%20(Slides).pdf (last accessed 10/20/2022).
[44] HSC section 127673.83(c)(2).
[45] Cal. Code Regs., title 11, section 820(j) [defining "bona fide researcher"].
[46] HSC section 127673.83(c)(1).

This section is based on the CURES regulation regarding "Eligibility for Access to Data from CURES."[47]

This regulation states the six different types of HPD data requests available under HPD's Data Use, Access and Release Program, each with their unique requirements. These six types are from HPD statute, and the requests are based on the following factors from statute: whether confidential or non-confidential HPD data (as defined in these regulations), whether limited identifiable data or directly identifiable data (i.e., "limited data" or "research identifiable data"), how the entity will receive the data (i.e., access through the Enclave or "direct transmission"), and whether the entity is a state agency or not.[48]

The purpose of this section is to give a clear overview of who is eligible for each of the six different types of data requests, and what regulatory section they need to follow to make the data request. This is to summarize this information in one place, so it is easier for a member of the public or state agency to know what regulatory section to follow.

The following goes into the specifics of the eligibility and the available data for each type of data request.

a. Section 97382, Subsection (a)

This subsection is about how anyone can request non-confidential HPD data. HPD statute has specific requirements about the release of confidential HPD data (i.e., record-level and/or identifiable data regarding patients and individual consumers).[49] However, the only thing that HPD statute states about non-confidential data is that it is exempt from the CPRA and that it can only be made available pursuant to HPD law.[50] Thus, in place of the CPRA, HCAI desires to create a procedure for any individual or organization to request and receive non-confidential HPD data. Generally, HCAI is required to produce and publicly make available data products and reports that do not have confidential HPD data[51], but if an entity wants something else, i.e., a custom report/product, that entity can make that request under this section.

---

[47] Cal. Code Regs., title 11, section 828.1.
[48] *See* HSC section 127673.81(c)(1) [regarding HPD data not being made available except pursuant to HPD law]; and sections 127673.82 and 127673.83 [regarding requirements for confidential HPD data, including obtaining and access through the Enclave].
[49] HSC sections 127673.8(d) and 127673.81(a) and (b); *see* HSC section 127673.82 [HPD statute refers to this confidential data as "nonpublic data" and specifically protects this data].
[50] HSC section 127673.81(c)(1).
[51] HSC section 127673.8(a).

Regarding eligibility, this subsection allows “any individual or organization” to request non-confidential HPD data. HCAI uses this language to have the broadest term possible to indicate that anything or anyone that has a separate legal existence can apply for HPD data. HCAI does not limit the type of entity who can apply for non-confidential data because HPD statute does not restrict the type of entities that can apply and because HCAI intends this section to be like the CPRA, which allows for broad access—giving “any natural person, corporation, partnership, limited liability company, firm, or association” access to public records in California.[52]

b. Section 97382, Subsections (b), (c) and (d)

These subsections are about confidential HPD data and specifically the following: subsection (b) about “limited data” through the Enclave, subsection (c) about “research identifiable data” through the Enclave, and subsection (d) for “direct transmission” of “standardized limited datasets.” Requirements for these types of data requests are specified in HPD statute.[53]

Regarding eligibility, like requests for non-confidential HPD data, these subsections allow “any individual or organization” to make these types of data requests for the same reasons stated for section 97382(a)—to indicate that anyone or anything can make these data requests. These three types of data requests have different requirements under statute, but HPD statute allows “qualified applicants” to make these types of data requests.[54] HPD statute does not have a definition for “qualified applicants,” but has a non-exhaustive list of entities that are “qualified applicants.[55] This indicates that HPD statute contemplated broad eligibility for these types of HPD data, especially since requesters still have to meet application requirements to receive confidential HPD data (as discussed below). For this reason, HCAI does not want to limit what entities can make these data requests.

Regarding section 97382(d) about the “direct transmission” of “standardized limited datasets, this subsection allows a requester to request the entire or just a part of a “standardized limited dataset.” This is to make clear that if a requester otherwise meets the requirements to obtain this data, it is not required that they obtain the entire dataset through this process. This is in recognition that a requester’s specific purpose for the data may not require all the data elements in a “standardized limited dataset” and is needed to better protect privacy.

---

[52] Cal. Gov. Code section 7920.520 [defining “person” for the CPRA]; and Cal. Gov. Code sections 7922.525 and 7922.530 [allowing every “person” to inspect public records or obtain copies of public records under the CPRA].
[53] HSC section 127673.83(b) and (c).
[54] HSC section 127673.83(b)(1) [regarding subsection (b)], (b)(2) [regarding subsection (c)], and (c)(1) [regarding subsection (d)].
[55] HSC section 127671(f)(5). This subdivision notes that “qualified applicants” just “includes” a variety of entities. Normally, “includes” does not create a restrictive definition in California law. (*Am. Nat'l Ins. Co. v. Fair Employment & Hous. Com.* (1982) 32 Cal.3d 603, 608.)

c. Section 97382, Subsection (e)

This subsection is about "direct transmission" of confidential HPD data that goes beyond requests for the "direct transmission" of "standardized limited datasets" in Section 97382(d).

Regarding the data at issue under this subsection, this subsection is based on the specific HPD statute about the "direct transmission" of "research identifiable data," HSC section 127673.83(c)(2). However, this subsection is broader than Section 127673.83(c)(2) and includes both "limited data" and "research identifiable data" forms of confidential HPD data. The reason for this is that HPD statute has a hole regarding the "direct transmission" of confidential HPD data: statute specifically provides requirements for the "direct transmission" of "standardized limited datasets" under certain conditions, and more stringent requirements for the "direct transmission" of "research identifiable data," but nothing generally about the "direct transmission" of other "limited data."[56] It does not make sense to allow "direct transmission" of the more sensitive and private "research identifiable data" but not "limited data" which is less sensitive. However, HPD statute gives HCAI discretion to develop procedures to release confidential data, as long as HCAI includes, at minimum, the privacy protection standards in Section 127673.83.[57] Pursuant to this discretion, HCAI chooses to treat the "direct transmission" of "limited data" like the "direct transmission" of "research identifiable data," since this has the most stringent requirements in HPD statute.

Regarding eligibility, pursuant to HPD statute,[58] this subsection limits this type of data request to "researchers" (defined by these proposed regulations and discussed above).

d. Section 97382, Subsection (f)

This subsection is about a specific type of data applicant, other state agencies. HPD statute states that HCAI may share HPD data with other state agencies pursuant to the Information Practices Act (IPA), Civil Code section 1798.24(e) which generally allows state agencies to share personal information about individuals with other governmental agencies.[59] This subsection implements this HPD statutory provision and allows state agencies to receive confidential HPD data pursuant to section 97400.

3. CCR, title 22, section 97384, "Data Application Fees"

Through Section 97384, with the exception of other state agencies, HCAI is requiring an application fee from applicants of HPD data. HCAI establishes this fee pursuant to HPD

[56] HSC section 127673.83(c).
[57] HSC section 127673.82(e).
[58] HSC section 127673.83(c)(2).
[59] HSC section 127673.83(d).

statute which requires HCAI to establish a "pricing mechanism for the use of nonpublic data."[60]

This fee is partially to sustain the HPD as the HPD does not have an established continual funding source[61] and processing applications will take substantial resources. The fee is also intended to prevent the spamming of data requests and to make sure that only authentic and serious requests are submitted for HCAI to process because HCAI has limited resources. HCAI exempts other state agencies from application fees because charging an application fee may create additional administrative hurdles for those agencies to get data. Also, the spamming rationale does not apply to other state agencies.

Section 97384(a) states the requirement of the application fee and states that HCAI will set the fees based on the type of HPD data being requested. The reason for different fees is that requests for confidential data or requests for "direct transmission" of data will require more scrutiny and more resources. HCAI does not set the fees in this proposed regulation as such prices do not have to be included in regulations.[62] HCAI will publish a separate fee schedule listing the application fees required.[63]

Subsection (b) notes that the fee needs to be submitted when the application is submitted and that an application will not be complete (and thus, not processed) unless such fee is paid. This is to make sure that data applicants pay the fee. The subsection goes on to state that the fee will be applied to the cost of the data if the application is approved and that otherwise, the fee is non-refundable. This is to clearly notify potential data applicants on what will happen with their application fees.

4. CCR, title 22, section 97386, "Review of Data Applications"

This section is necessary to provide HCAI the ability to go beyond the data application requirements to properly evaluate data applicants and data requests. This also provides notice to data applicants what discretionary actions HCAI may take to assess data applications beyond the requirements in later proposed regulations, so applicants know what to expect. These potential actions are general because requests will be unique and HCAI will have to decide what to do on a case-by-case basis based on the circumstances of a request.

---

[60] HSC section 127673.82(c).
[61] HSC section 127674 [noting that no more General Fund moneys will be appropriated for the HPD and that the HPD is allowed to collect fees and raise revenue].
[62] Cal. Gov. Code section 11340.9 [the California formal rulemaking requirements do not apply to "a regulation that establishes or fixes rates, prices, or tariffs"].
[63] *See* HSC section 127674(f)(2) [regarding HCAI "establishing the user fee schedule…"].

Subsection (a) allows HCAI to request further information from the applicant beyond the regulatory application requirements. This is necessary if the information provided is unclear, insufficient, or raises issues to investigate to make sure that it is appropriate to release HPD data to an applicant, particularly confidential HPD data, and that HPD data is properly protected, if necessary.

Subsection (b) allows HCAI to seek input or recommendations from the HPD Data Release Committee. Under HPD statute, the Committee must review and provide recommendations on some HPD confidential data requests.[64] HPD statute also allows HCAI to seek recommendations from the Committee on other data applications.[65] This regulation gives HCAI discretion to send any HPD data request to the Committee when it determines it is necessary.

Subsection (c) allows HCAI to seek input from any other source regarding a data application. This is necessary if there are unique circumstances about the requester, the data requested, or the uses of data that HCAI needs more information about in order to properly screen a requester or data use and make sure HPD data is properly protected. The subsection lists potential entities HCAI may contact including the public (if a request may affect the public at large or may be controversial), regulatory bodies (if a data use touches upon antitrust/competitiveness issues, or otherwise affects a regulated business), other state agencies (if a request could impact them), the HPD Advisory Committee (like the public and for general advice on whether a data use is appropriate), or the sources of data (in case a request may infringe on any agreements through which HCAI received the data).

5. CCR, title 22, section 97388, "General Reasons to Deny Data Applications"

This section is necessary because it provides notice to the public regarding when HCAI is required to deny data requests and when it may, in its discretion, deny data requests. This allows potential requesters to review the possible reasons for denial and decide whether to apply or not or how to frame their data applications better, which will save HCAI resources when reviewing applications. This also places limitations on HCAI's ability to deny applications and that it must have reasonable grounds to deny applications.

These are "general" reasons because they apply to all or many data request types or are grouped in simpler categories of data requests (e.g., all requests for confidential HPD data, or all requests for the "direct transmission" of confidential data). Unique requirements for each type of data request are stated in the later proposed regulations about the specific type of data request (proposed sections 97392 to 97400).

[64] HSC section 127673.84(d)(1); and HSC section 127673.83(b)(2)(A) and (c).
[65] HSC section 127673.84(d)(1).

a. Section 97388, Subsection (a)

Subsection (a) notifies the public about the scope of this section—that it applies to all requests for HPD data. It also notifies the public that specific types of HPD data requests may have their own grounds for denial. Specific reasons for denial, based on the type of data request, are included in the specific regulations about those data requests.[66] This subsection is needed to provide clarity on the applicability of this section and that other sections may also apply regarding reasons for denial.

b. Section 97388, Subsections (b) and (c)

Subsections (b) and (c) discuss that HCAI may deny requests in "whole or in part." The reason for this is that certain aspects of a data request may be appropriate—for example, it may be inappropriate to release a subset of data, or that the type of data is approved but the manner in which the requester wants it (e.g., transmitted to them) is not. This gives HCAI flexibility to approve data requests to a certain extent instead of rejecting them outright and requiring new applications, which will save HCAI and requesters time and resources.

c. Section 97388, Subsection (b)

Subsection (b) states the circumstances in which HCAI must deny HPD data requests when it determines the circumstances are present. Thus, HCAI will be required to analyze each data request for these issues before releasing HPD data. This also provides clarity and notice to potential requesters.

i. Subsection (b)(1)

This subsection states the obvious that HCAI must deny a request if state or federal law somehow prohibits the requested disclosure. This is akin to the exemption under the CPRA[67] that allows a state agency to not disclose public records when "prohibited pursuant to federal or state law."[68]

ii. Subsection (b)(2)

This subsection is in regard to data that HCAI may receive outside of its normal data collection processes from mandatory and voluntary submitters.[69] This may include agreements with the federal government and other state agencies to provide their data to the HPD. Those agreements (based on laws that apply to those entities or based on

[66] *See* proposed regulations, Cal. Code Regs., title 22, sections 97390 to 97400.
[67] Cal. Gov. Code sections 7920.000, *et seq*.
[68] Cal. Gov. Code section 7927.705.
[69] *See* HSC section 127673(b) [regarding collection of health care data from mandatory and voluntary submitters, as defined].

their policies) may prevent HCAI from disclosing data either in whole or in part. This subsection recognizes these constraints and notifies the public about this.

iii. Subsection (b)(3)

This subsection makes sure that HCAI will evaluate the safety or privacy risk to Californians and prevent any data release that could reasonably harm Californians. The specific language of this subsection is adapted from HSC section 128766(c), another HCAI data program, which has a similar requirement.

This subsection is partially based on the right of privacy for individuals in the California Constitution[70] and, accordingly, the heavy emphasis that HPD statute places on protecting patient and individual consumer data.[71] For example, HPD statute states that HCAI's data access and release regulations must "be designed to recognize a patient's right of privacy…."[72] This subsection recognizes this right of privacy and the effect that data release may have on individuals. Thus, this subsection states that HCAI will deny requests if it determines that release of the data will create an unreasonable risk to the privacy of *any* individual, including beyond patients and consumers.

This subsection also notes that HCAI will not release data if the release creates an unreasonable risk to an individual's safety. This is in recognition that the safety of individuals could be at risk if personal information is disclosed. For example, a requester may ask for personal data about doctors who practice reproductive health, which could be used to target the doctors for violence or harassment.

iv. Subsection (b)(4)

This states that HCAI will deny a data request if it is inconsistent with the goals of the HPD, which are stated in statute.[73] The reason for this is that data collected under HPD law for specific purposes must be used for those purposes and in no way that undermines those purposes.

v. Subsection (b)(5)

This is only about confidential HPD data—that is record-level or identifiable data about patients and individual consumers.

Parts (A) and (B) of this subsection are about requests for which HCAI determines that a requester asked for confidential data that is not needed for the requester's proposed

[70] Cal. Const. Article I, section 1.
[71] HSC sections 127673(b)(3), 127673.5(a)(2), 127673.8(d), and 127673.81(a) and (b).
[72] HSC section 127673.82(e).
[73] HSC section 127671.

use. This is a statutory prohibition that limits a data requester from obtaining more than "the minimum amount of potentially identifiable data necessary" for their use.[74] There could be two circumstances here that subparts (A) and (B) address: either (A) when confidential HPD data is not needed for a purpose, or (B) the requester asks for more than the minimum amount of confidential data than they really need.

Part (C) of this subsection deals with the circumstance in which a requester wants unnecessary personnel to be able to observe, control or use the data. As discussed later, a requester potentially will have several individuals working with the confidential HPD data for its use. This denial reason is to make sure that the requester only uses the minimal amount of personnel to limit the disclosure of confidential information. This requirement is based on a similar requirement in HIPAA.[75]

Part (D) of this subsection, regarding mandatory denial for using, observing, controlling or storing confidential HPD data outside the United States of America, is needed because once the HPD data leaves the United States of America, it would be incredibly difficult or impossible for HCAI to take action to retrieve or protect the data. If a data user misused the HPD data outside the United States, HCAI would have to navigate a foreign legal system, which could have different views about individual privacy or be hostile to the United States of America, and HCAI would be less likely to be able to take the steps necessary to prevent misuse of the data based on the complexity and cost of taking legal action in another country.

vi. Subsection (b)(6)

This subsection, which includes parts (A) and (B), applies only to data applications for the "direct transmission" of confidential HPD data, including "standardized limited datasets." HPD statute is the most protective of these types of data requests as it poses the most security and privacy risks.[76] For these reasons, these types of data requests have additional requirements that must be met for an application to be approved.

Part (A) of this subsection is about the HPD statutory requirement for HCAI to establish the Enclave, or the "secure research environment" for entities to virtually access HPD data.[77] The intent of HPD statute and HCAI is to have most data requesters receive confidential HPD data through the Enclave,[78] where confidential data can be better monitored, controlled, and protected compared to sending data copies to recipients. Data recipients will be unable to take identifiable or record-level consumer data from the

[74] HSC section 127673.83(a).
[75] Fed. Code Regs., title 45, section 164.514(d)(2) [regarding individuals to have access to confidential data when necessary].
[76] *See* HSC section 127673.83(c).
[77] HSC 127673.82(d).
[78] HSC section 127673.83(c) [stating that HCAI "shall limit release or transmittal of personal information outside the secure environment," i.e., the Enclave].

Enclave and will only be able to observe and use that data within the Enclave. This mandatory reason for denial is in recognition that statute and HCAI desires data users to use the Enclave when possible and that requesters should not be able to obtain copies of confidential HPD data when they can reasonably use the Enclave instead.

Part (B) of this subsection is from HPD statute, which requires entities, for the "direct transmission" of confidential HPD data, to have "data security [that] meet the standards that" HCAI determines.[79] HCAI also wishes to apply this to state agency requests for the "direct transmission" of confidential HPD data, even though this is controlled by a separate HPD statutory section that does not explicitly have this data security requirement.[80] HPD statute gives authority to do this as the HPD statutory requirements are only minimum requirements which HCAI can add to[81] and because this is consistent with HPD statute's requirement that HCAI develop regulations to "ensure that the privacy, security, and confidentiality of consumers' individually identifiable health information is protected."[82] HCAI believes that the same requirements should apply to all entities, whether a state agency or not, for "direct transmission" of confidential HPD data as all entities are vulnerable to data breaches.[83] This subsection implements this and states that HCAI will deny a data application for "direct transmission" of confidential HPD data if the applicant's data security does not meet the standards HCAI developed in these regulations (proposed section 97406).

vii. Subsection (b)(7)

This subsection, regarding mandatory denial for using HPD data for determinations about the health care of individuals, including about treatment, eligibility, coverage, or similar purposes, is a specific prohibition from HPD statute.[84] It is included here for clarity and to adequately provide notice to potential data requesters.

d. Section 97388, Subsection (c)

This subsection gives HCAI discretionary authority to deny data requests when it determines there is good cause to do so. This gives HCAI flexibility to deny a data request based on the unique circumstances of a requester, the data requested, the data use, or other factors. However, this subsection prevents HCAI from making arbitrary or

[79] HSC section 127673.83(c)(1) and (2).
[80] HSC section 127673.83(d).
[81] HSC section 127673.82(e) [stating HCAI "shall include at least the privacy protection standards specified in Section 127673.83"].
[82] HSC section 127673.5(a)(2).
[83] For instance, the alleged theft of confidential data from the California Department of Finance in December 2022. *See* Lindsey Holden, *California investigates cybersecurity incident at Department of Finance*, The Sacramento Bee, (December 12, 2022), https://www.sacbee.com/news/politics-government/capitol-alert/article269915257.html (last accessed 1/23/2023).
[84] HSC section 127673.81(d).

capricious decisions by requiring it to have "good cause," or in other words, "reasonable grounds and good faith."[85] This subsection is akin to the CPRA's statutory exemptions, which state agencies have discretion to use or not based on the circumstances.[86]

Subsection (c) goes on to give examples of what may constitute good cause to deny an HPD data request so requesters are put on notice regarding what could prevent them from receiving HPD data and also to give guidance to HCAI decisionmakers.

i. Subsection (c)(1)

This subsection notes that there would be good cause for denial if a requester does not comply with the regulations for the HPD Data Use, Access, and Release Program. This is to make sure that requesters follow the requirements set forth by HCAI for the HPD.

ii. Subsection (c)(2)

This subsection notes that there would be good cause for denial if a requester does not comply with HPD data submission requirements. This is in regard to organizations who are mandated by law to submit data to the HPD and fail to do so or fail to do so properly. If an organization fails to live up to its obligations to the HPD, it may not be able to benefit from the HPD.

iii. Subsection (c)(3)

This subsection is based on the catchall exemption in the CPRA, which is supposed to be applied to the "facts of the particular case."[87] This is a balancing test regarding whether the public interest would be served better with disclosure versus withholding of the data. HCAI incorporates this CPRA exemption because this exemption is well-established and thus, the State and the public have a good understanding of what this means. This standard can readily be applied to unique cases where there may be countervailing public interests. For example, it may be beneficial to release some contractual pricing and rates information to increase transparency and to disclose issues in health care, but such disclosure may also lead to anti-competitive behavior and may be detrimental. This subsection allows for a balancing of these or similar issues and for HCAI to withhold data or limit disclosure.

However, HCAI altered the balancing test by reversing it (i.e., the public interest in disclosure must outweigh the interest in non-disclosure instead of vice versa) and changing "clearly outweigh" to just "outweigh." The reason for this alteration is that the

[85] *People v. Accredited Sur. Cas. Co.* (2014) 230 Cal.App.4th 548, 559-60 [defining "good cause"].
[86] *Amgen Inc. v. Health Care Services* (2020) 47 Cal.App.5th 716 ["The exemptions in [the CPRA] 'are permissive, not mandatory: They allow nondisclosure but do not prohibit disclosure.'"].
[87] Cal. Gov. Code section 7922.000.

CPRA favors disclosure over withholding, but unlike many public records, HPD data consists or will consist of an immense amount of sensitive and private information about Californians collected and aggregated largely without their permission. Thus, since HCAI needs to be more protective of the data than an ordinary public record, it seems HCAI should be more cautious in disclosing information compared to the CPRA. Statute appears to recognize this as HPD statute exempts HPD data from the disclosure requirements of the CPRA.[88]

6. CCR, title 22, sections 97390 to 97400, General Application Requirements

The following discuss the same or similar application requirements to receive HPD data which are stated in the different proposed regulations for the six different types of data requests. HCAI requests this information in applications so it can properly screen and more efficiently process applications. Many of the application requirements are repeated in each regulation to provide more clarity to potential data requesters and HCAI staff. Having all the requirements for a particular data request in one section will prevent readers from having to go back and forth and will hopefully prevent mistakes and confusion, especially since some of the types of data request have unique requirements.

Some of the application requirements are the same for all six types of data requests, but some requirements are absent, slightly differ, or are completely different. HCAI discusses the same or similar application requirements for the types of data requests here, so it is easier to compare and understand. Unique application requirements will be discussed later as they require more extensive explanation.

a. Sections 97390(a), 97392(a), 97394(a), 97396(a), 97398(a), and 97400(a), Electronic Applications

All of the data request regulations require that a requester apply for HPD data electronically. This is required because electronic submission is the most efficient and convenient method for HCAI to receive applications and HCAI expects that the vast majority of requesters will have online access, especially since one needs online access to access the Enclave. HCAI intends to have an electronic form that incorporates all of the specific application requirements based on the type of data request.

b. Sections 97390(a)(1), 97392(a)(1), 97394(a)(1), 97396(a)(1), 97398(a)(1), and 97400(a)(1), "Date of Application"

This application requirement is the same as for the CURES regulations.[89]

[88] HSC section 127673.81(c)(1).
[89] Cal. Code Regs., title 11, section 828.5(c)(1).

All these subsections require a date of the application as later regulations create deadlines for the review of applications based on when a complete application was submitted.[90] HPD statute requires HCAI to "maintain information about requests and the disposition of requests and shall develop processes for the timely consideration and release of nonpublic data."[91] For the purpose of keeping track of requests, a date is needed especially to determine if HCAI is timely processing them.

c. Sections 97390(a)(2), 97392(a)(2), 97394(a)(2), 97396(a)(2), and 97400(a)(2) "Name of the Data Applicant, and Whether an Individual or Type of Organization"

All these subsections require the name of the data applicant and whether an individual or the type of organization. HCAI needs this information to properly identity the requester and to verify or investigate the requester if necessary.

For Section 97400(a)(2), regarding state agency requests, entity type is not asked for because this section is only for state agencies.

Section 97398(a), regarding "direct transmission" of confidential HPD data, does not have this requirement because only an individual researcher can make this data request and is addressed by Section 97398(a)(2) regarding the applicant's contact information.

d. Sections 97390(a)(3), 97392(a)(3), 97394(a)(3), 97396(a)(3), and 97400(a)(3) "Whether the Data Applicant Submits Data to HPD"

These subsections require the data applicant to identify whether it submits data to the HPD. This will allow HCAI to more easily check whether the applicant is complying with HPD statutes and regulations when determining whether to approve or deny the application under proposed section 97388(c)(2). HCAI is also required to establish a data "user fee schedule and fee waivers" for HPD data and HPD statute requires HCAI to "make considerations" regarding fees for "data submitters."[92] There may be reduced HPD data prices for data submitters, and this will make it easier for HCAI to identify what data fees should be assessed if an application is approved.

The similar requirement in Section 97398(a)(5), for "direct transmission" of confidential HPD data, is not discussed here because this type of data request is the most unique and requires additional explanation (see below).

[90] *See* proposed regulation, Cal. Code Regs., title 22, section 97410(a)(1) [written notice regarding HCAI decisions on HPD data applications must be sent within 60 days of the application].
[91] HSC section 127673.82(g).
[92] HSC section 127674(f)(2).

e. Sections 97390(a)(4), 97392(a)(4), 97394(a)(4), 97396(a)(4), 97398(a)(2) and 97400(a)(4), Applicant Contact Information

These subsections ask for contact information of the data applicants so that HCAI knows how to contact the applicant about their application and requests different ways to contact the applicant in case one method does not work.

For applicants who are organizations, HCAI requests the name and title of the organization's "authorized representative" as defined in these proposed regulations.[93] The reasons for an "authorized representative" are explained above regarding the regulatory definition. The identity of this person is needed so HCAI knows who it is dealing with and can attempt to reach this person when needed to process the application.

For section 97398(a)(2), regarding "direct transmission" of confidential HPD data, this section just seeks information about the requester, who can only be an individual per statute.[94]

f. Sections 97390(a)(5), 97392(a)(5), 97394(a)(5), 97396(a)(5), 97398(a)(6) and 97400(a)(5), Description of the Requested Data

This subsection requests the applicant to describe in detail the data it wants from HPD. HCAI asks for a detailed description so it can see whether it has that data or whether it can be created with existing data (for example through data linkage, or aggregation of record-level data). This subsection is needed so HCAI has sufficient information in the beginning to determine whether it has (or can have) the data the requester wants without having to follow-up with the requester. This will make the process more efficient and convenient.

Regarding time period for confidential HPD data requests (sections 97392(a)(5), 97394(a)(5), 97396(a)(5), 97398(a)(6) and 97400(a)(5)), HCAI also asks for the time period for the data. Based on the years of experience HCAI has had providing data to the public, HCAI knows that this is needed to make the process more efficient. HPD is collecting an immense amount of confidential HPD that span many years. By having the requester state a time period, HCAI can more efficiently determine whether it has the data (or can have it). This is not required for non-confidential requests because those requests can theoretically request many different types of data for which a time period does not apply.

Regarding data elements for confidential HPD data requests, HCAI also asks for a list of each confidential data element desired and an explanation of why the requester wants

[93] See above and proposed regulation Cal. Code Regs, title 22, section 97380(b).
[94] HSC section 127673.83(c)(2).

that element. HPD statute (and which is a common limitation[95]) limits disclosure "to the minimum amount of potentially identifiable data necessary for an approved project."[96] This subsection is needed for this statutory limitation—that HCAI has sufficient information to analyze whether the request is only asking for the minimum amount of data necessary. With this information, HCAI can determine whether to deny, in whole or in part, a data application that asks for unnecessary data elements per proposed section 97388(b)(5) (discussed above).

Section 97396(a)(5), regarding "direct transmission" of "standardized limited datasets," HCAI also requests for the requester to identify the "standardized limited dataset" it wants, but retains the requirement to explain the need for every confidential data element. As defined, "standardized limited datasets" will be created for "types of purposes specified by [HCAI],"[97] but, as discussed above,[98] a requester may not need all the confidential data elements in such a dataset for a specific purpose. To make it more efficient to process these types of requests, HCAI also requests a requester to list the confidential data elements in a "standardized limited dataset" it is not requesting.

g. Sections 97390(a)(6), 97392(a)(6), 97394(a)(6), 97396(a)(6), 97398(a)(7) and 97400(a)(6), Data Use

This application requirement is similar to CURES regulations which requests the purposes and objectives of the project using CURES data.[99]

Generally, these subsections ask for the proposed use of the HPD data, i.e., why the applicant wants the requested HPD data; and how that will be consistent with the HPD goals and purposes. This information is needed to evaluate whether HCAI is required to deny a data application for not being consistent with the HPD goals per proposed section 97388(b)(4) (discussed above). This is also requested so HCAI can evaluate whether there are countervailing public interests against release pursuant to proposed section 97388(c)(3) (discussed above). For example, there are antitrust and anti-competitiveness concerns with the release of business/contractual pricing information. By knowing what the use of the data will be, HCAI will be able to assess whether it is in the best interests of California to release the data.

For all applications for confidential HPD data, as part of the applicant's data use explanation, HCAI also requests the entity to describe the "public data products" (as defined in these regulations) that may be created with the requested data and how such

---

[95] *See* Code of Fed. Regs., title 45, section 164.514(d)(4)(i) ["a covered entity must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made…].
[96] *See* HSC section 127673.83(a) [regarding access through the Enclave].
[97] HSC section 127673.83(c)(1).
[98] See Section IV.2.b above regarding requests for "direct transmission" of "standardized limited datasets."
[99] Cal. Code Regs., title 11, section 828.6(c)(11)(A)(1).

products will be disclosed. HCAI needs to know this to properly assess the risks and issues that may come from products that are created with confidential information and determine if the application needs to be denied in whole or in part, or if other issues must be considered (such as what data use agreement provisions are needed and whether the proposed regulations on public data products, Section 97416 apply).

These subsections also incorporate HPD statute's unique requirements regarding the use of confidential HPD data for specific data request types.[100] Thus, each type of data request has a unique application requirement about data use which will be discussed below.

i. Non-Confidential Data Applications, Section 97390(a)(6)

For non-confidential data, this subsection just generally asks why the entity wants the data and how it will be consistent with HPD goals as explained above.

ii. "Limited Data" Through the Enclave Applications, Section 97392(a)(6)

HPD statute only allows access to "limited data" through the Enclave "for research and analysis purposes consistent with program goals."[101] This subsection tracks this statutory language and requires an entity to describe in its application the research or analysis purpose and how it will be consistent with HPD goals. HCAI needs this information to determine whether the application meets statutory requirements and can be approved.

iii. "Research Identifiable Data" Through the Enclave Applications, Section 97394(a)(6)

HPD statute only allows access to "research identifiable data" through the Enclave "for research projects that offer significant opportunities to achieve program goals."[102] This subsection tracks this statutory language and requires an entity to describe in its application its "research project" and how it will "offer significant opportunities to achieve [HPD] goals." HCAI needs this information to determine whether the application meets statutory requirements and can be approved.

iv. Applications for the "Direct Transmission" of "Standardized Limited Datasets", Section 97396(a)(6)

HPD statute allows HCAI to develop "standardized limited datasets" "for types of purposes specified by" HCAI.[103] This subsection tracks this statutory language and

[100] HSC section 127673.83(b), (c) and (d)
[101] HSC section 127673.83(b)(1).
[102] HSC section 127673.83(b)(2).
[103] HSC section 127673.83(c)(1).

requires an entity, for "direct transmission" of these datasets, to describe its data use and how it is consistent with the purpose of the "standardized limited dataset" HCAI specified. HCAI needs this information to determine whether the application meets statutory requirements and can be approved.

v. Applications for the "Direct Transmission" of Confidential HPD Data, Section 97398(a)(7)

HPD statute only allows "direct transmission" of confidential HPD data "for research projects that offer significant opportunities to achieve program goals."[104] This subsection tracks this statutory language and requires an entity to describe in its application its "research project" and how it will "offer significant opportunities to achieve [HPD] goals." HCAI needs this information to determine whether the application meets statutory requirements and can be approved.

vi. State Agency Applications for Confidential HPD Data, Section 97400(a)(6)

As discussed above, HPD statute allows HCAI to share confidential HPD data with other state agencies pursuant to Civil Code section 1798.24(e), which is part of the IPA.[105] Civil Code section 1798.24(e) allows a state agency to share personal information about individuals with other state agencies if the sharing is needed for the other state agency:

> "to perform its constitutional or statutory duties, and the use is compatible with a purpose for which the information was collected."[106]

This subsection tracks this statutory language and requires a state agency requesting confidential HPD data to explain why it wants the data, how the data will be used for purposes consistent with the program, and how the data is necessary for the state agency to perform its constitutional or statutory duties. HCAI needs this information to determine whether the application meets statutory requirements and can be approved.

h. Sections 97390(a)(7), and 97400(a)(7), How to Receive HPD Data

Two types of HPD data requests, for non-confidential HPD data and state agency requests, do not include a method of data receipt (i.e., either "data transmission" or through the Enclave). These subsections request the applicant to state how it wants the

[104] HSC section 127673.83(c)(2). This statute is only about "research identifiable data" but, as discussed above (for Section 97382(e)), HCAI is implementing this section for customized "limited data" too.
[105] HSC section 127673.83(d).
[106] Cal. Civil Code section 1798.24(e) also requires that the data "use or transfer is in accordance with Section 1798.25" which requires HCAI to "keep an accurate accounting of" the data disclosure.

data. This will allow HCAI to properly calculate data fees, check if the request is feasible, and plan for data release. This will make the data release process more efficient and prevent surprises to the requester.

i. Sections 97390(a)(8), 97392(a)(7), 97394(a)(7), 97396(a)(8), 97398(a)(9), and 97400(a)(8), Length of Time Wanted or Needed with HPD Data

These subsections require the requester to state how long they want or need the HPD data.

i. Regarding Access via the Enclave

For section 97390(a)(8), regarding non-confidential HPD data, this application requirement is only if the requester wants access to the data through the Enclave. Sections 97392(a)(7) and 97394(a)(7) are just about accessing confidential HPD data through the Enclave. Section 97400(a)(8), for state agency requests, Enclave access is a way to receive HPD data.

By having information about how much time the applicant wants or needs the data in the Enclave, HCAI will be able to price the data request better and more efficiently; and be able to assess its available resources and thus, determine to what extent HCAI can meet the request.

ii. Regarding "Direct Transmission" of Confidential HPD Data

To best protect confidential HPD data, if "directly transmitted" to them, HCAI will not allow an applicant to obtain and keep confidential HPD data for more time than the applicant needs it. The longer an entity has HPD data, the more risk there is that it will be improperly used or disclosed at some point. Also, HCAI needs to know the anticipated length of time to properly price the HPD data release and also to determine what additional protections are needed, if any, in data use agreements which are required by HPD statute.[107] For these reasons, these application requirements (sections 97396(a)(8), 97398(a)(9), and 97400(a)(8) [requests for "direct transmission" of confidential data]) request how long the requester needs the confidential HPD data in its possession.

j. Sections 97390(a)(9), 97392(a)(13), 97394(a)(16), 97396(a)(16), 97398(a)(19), and 97400(a)(14), Signature

These subsections require a signature of the data applicant, if an individual, or of the authorized representative, certifying the information in the application and date of signature. This is so that HCAI ensures that it receives truthful and accurate information, and that the requester knows that they must make sure to provide accurate and truthful information to HCAI.

[107] HSC section 127673.83(a).

7. CCR, title 22, sections 97392 to 97400, Confidential HPD Data Application Requirements

The following discuss the same or similar application requirements to receive confidential HPD data. Just like for the general application requirements, HCAI requests this information so it can properly review and more efficiently process applications. Many of the application requirements are repeated in each regulation for confidential HPD data to provide more clarity to potential data requesters and HCAI staff. Having all the requirements for a particular data request in one section will prevent readers from having to go back and forth and will hopefully prevent mistakes and confusion, especially since some of the types of data request have unique requirements.

HCAI discusses the same or similar application requirements for the types of data requests here, so it is easier to compare and understand. Some application requirements will be discussed later as they require more extensive explanation.

a. Sections 97396(a)(7), 97398(a)(8) and 97400(a)(7), Rationale for "Direct Transmission" of Confidential HPD Data, Instead of Through the Enclave

These three subsections are about requests for "direct transmission" of confidential HPD data instead of accessing it the through the Enclave (i.e., section 97396 regarding "direct transmission" of "standardized limited datasets," section 97398 regarding "direct transmission" of "confidential HPD data" and possibly section 97400 through which state agency may request "direct transmission").

These subsections require an explanation of why the data requester wants "direct transmission" of the data instead of accessing it through the Enclave. As discussed above, per proposed section 97388(b)(6), HCAI will be required to reject a data application if an entity does not need "direct transmission" of the data and can achieve the same purposes through the Enclave. This application requirement is so HCAI can determine this.

b. Sections 97392(a)(8), 97394(a)(8), 97396(a)(9), 97398(a)(10), and 97400(a)(9), List of Outside Data

This application requirement is based on prohibitions in HIPAA and a different HCAI program, based on HSC section 128766, regarding the release of data without direct identifiers, i.e., "limited data." HIPAA prohibits "limited data" recipients from "identify[ing] the information or contact[ing] the individuals."[108] The HCAI statute prohibits "limited data" recipients from "reidentify[ing] or attempt[ing] to reidentify" the data.[109] It is

[108] Fed. Code Regs., title 45, section 164.514(e)(4)(ii)(C)(5).
[109] HSC section 128766(b).

problematic for a data recipient to use outside data to make "limited data" more identifiable because it increases the privacy and security risks without the data provider knowing.

Based on the above, these subsections require the HPD confidential data requester to provide a list of any data from outside the HPD that it intends to use or link with confidential HPD data. HCAI requests this information to address the issue discussed above and determine whether the requester will make the confidential HPD data more identifiable or sensitive. Based on this information, HCAI can assess whether to deny the data request, to prohibit the use/linkage of outside data, or other measures to mitigate any increased privacy or security risk (such as through the required data use agreement).

c. Sections 97392(a)(9), 97394(a)(9), 97396(a)(10), 97398(a)(11), and 97400(a)(10), List of Contractors and Individuals and Physical Location

These subsections require data applicants to list all contractors and individuals who will work with the confidential HPD data, the physical locations where they will work with the data, and the position/role of the individual/contractor regarding the data.

A similar application requirement is in the CURES regulations.[110] This application requirement is also based on HIPAA and a different HCAI data program, based on HSC section 128766, regarding the release of "limited data." HIPAA requires a "limited data" provider to "[e]stablish who is permitted to use or receive the limited data set" from the data recipient.[111] As part of HCAI's program pursuant to HSC 128766, HCAI requests data recipients to identify individuals and contractors who will use the "limited data." HCAI wishes to adopt a similar approach for HPD for the following reasons.

First, HPD statute requires that "[e]ach person who accesses or obtains nonpublic personal [HPD] data shall sign a data use agreement."[112] For this reason, HCAI needs a list of all individuals and contractors of the data recipient, so HCAI knows everyone who is required to execute a data use agreement.

Second, HIPAA requires entities to only disclose confidential data to those who need access to that data "to carry out their duties."[113] This minimizes privacy intrusions and security risks by only allowing the minimum amount of people to access confidential HPD data. This application requirement requires a data applicant to list everyone who will work with the confidential HPD data and their roles/positions regarding the data. This information will allow HCAI to assess whether only the minimum and necessary personnel will use the confidential data.

[110] Cal. Code Regs., title 11, section 828.6(c)(9).
[111] Fed. Code Regs., title 45, section 164.514(e)(4)(ii)(B).
[112] HSC section 127673.83(a).
[113] Fed. Code Regs., title 45, section 164.514(d)(2).

Third, by knowing who will use or control confidential HPD data, whether a contractor entity or an individual, HCAI can assess whether those persons pose privacy and security risks. For example, HCAI may know, from previous data requests with other data recipients, that a certain contractor does not properly secure confidential data or has misused confidential data.

Regarding physical location, a reason for denial under proposed section 97388(b)(8) is that confidential HPD data will be used outside the United States of America (which is explained above). To determine whether this may occur, these subsections require the applicant to state where individual data users will use the data. Also, by knowing the physical location, HCAI can assess potential security and privacy risks better. For example, there are different issues depending on whether individuals work in an office location or from their homes.

d. Sections 97394(a)(10), 97396(a)(11), and 97398(a)(12), Expertise with Privacy Protection and the Analysis of Large Sets of Confidential Information

These subsections implement a statutory minimum requirement[114] for these types of HPD data requests (i.e., Section 97394 for "research identifiable data" in the Enclave; Section 97396 for "direct transmission" of "standardized limited datasets"; and Section 97398 for "direct transmission" of confidential HPD data). Specifically, for these types of HPD data requests, HPD statute requires that the "requester has documented expertise with privacy protection and with the analysis of large sets of confidential data."[115]

To review applications for this statutory requirement, through these subsections, HCAI will require the applicant, if an individual, or the "authorized representative" to describe their "expertise with privacy protection and with the analysis of large sets of confidential information" and to provide documents in support of their expertise as statute requires "documented expertise." HCAI will review this information and determine if the requester meets this statutory requirement on a case-by-case basis.

For organizational applicants, the focus is on an individual, the "authorized representative," having "documented expertise" instead of the organization as a whole because although an organization may have this expertise, the "authorized representative," i.e., the individual in charge of the confidential HPD data, may personally lack that expertise. HCAI believes it better meets HPD statutory intent and better protects the confidential data if the "authorized representative" has this expertise since they will be responsible for the HPD data. This is supported by HCAI statute that switches from the term "qualified applicant" when discussing data applicants to the term

[114] *See* HSC section 127673.82(e) [stating that HCAI data release policies or regulations "shall include at least the privacy protection standards specified in Section 127673.83"].
[115] HSC section 127673.83(b)(2)(C), (c)(1), and (c)(2).

"requester" when discussing the person who needs to meet this statutory requirement.[116]

Proposed section 97398(a)(12) also has additional requirements specific for this type of data request and will be discussed below.

e. Sections 97392(a)(10), 97394(a)(11), 97396(a)(12), 97398(a)(13), and 97400(a)(11), History of Data Breaches

For all confidential HPD data requests, these subsections require a data applicant to describe their data breaches of confidential information in the past seven years which the applicant or their "authorized representative" caused or was responsible for and a description of corrective measures after such incidents.

As noted above, a mandatory reason for denial is if disclosure of the confidential HPD data would "create an unreasonable risk to individual privacy or security" (per proposed section 97388(b)(3)). Having this information will allow HCAI to assess whether there is an "unreasonable risk" in releasing confidential data to the applicant. HCAI asks for seven years to match the "History of Theft/Fraud Convictions" section below (and which is explained there). HCAI also requires incidents by the applicant and their "authorized representative" so that both the organization and the individual in charge can be assessed. HCAI also requests corrective measures taken to determine whether any issues have been fixed or whether the applicant is willing to fix issues.

HCAI requests this information from the data applicant directly as they would be in the best position to know this. Also, as noted in the IPA, state policy is to collect information "to the greatest extent practicable directly from… the subject of the information rather than another source."[117] If done without the applicant, HCAI may miss relevant information for its review.

HCAI does not expect to do outside verification or research about this for every data applicant but may do so on a case-by-case basis. Since this is the case, it is important for the data applicant to provide this information so any problematic incidents can be reviewed and addressed so HCAI can mitigate problems in the beginning and to assure the public that their personal information will be protected.

HCAI does not require this information for every person who may use, view or control confidential HPD data per a data application because it did not want to collect so much information about individuals. HCAI addresses this issue by requiring data applicants to conduct thorough background checks on its personnel when requesting "direct

[116] HSC section 127673.83(b)(2)(C), (c)(1), and (c)(2) [noting that confidential data can be provided to "qualified applicants" but that the "requester" must have this expertise].
[117] Cal. Civil Code section 1798.15.

transmission “of confidential HPD data and keeping records of those checks—see later discussion regarding proposed section 97406(c)(1).

f. Sections 97392(a)(11), 97394(a)(12), 97396(a)(13), 97398(a)(14), and 97400(a)(12), History of Fraud/Theft Convictions or Civil Actions

For all confidential HPD data requests, these subsections require a data applicant and their “authorized representative,” to disclose “criminal convictions or substantiated violations of federal law regarding fraud, theft, data breach, data misuse, or related offenses, in the past seven years.” These subsections go on to state what “substantiated violations” include, such as administrative penalties and civil judgments.

As noted above, a mandatory reason for denial is if disclosure of the confidential HPD data would “create an unreasonable risk to individual privacy or security” (per proposed section 97388(b)(3)). Having this information will allow HCAI to assess whether there is an “unreasonable risk” in releasing confidential data to the applicant—that is, whether there is a risk, based on recent history, that data will be stolen or misused. This information is requested for seven years because California law limits background check reports on individuals to seven years.[118] This applies to both the applicant and their “authorized representative” so that both the organization and the individual in charge can be assessed.

HCAI does not require this information for every person who may use, view or control confidential HPD data per a data application because it did not want to collect so much sensitive information. HCAI addresses this issue by requiring data applicants to conduct thorough background checks on its personnel when there is “direct transmission” of confidential HPD data and keeping records of those checks—see later discussion regarding proposed section 97406(c)(1).

HCAI requests this information directly from the data applicant for the same reasons discussed above regarding “history of data breaches.” Also, like above, HCAI does not expect to do outside verification or research about this for every data applicant but may do so on a case-by-case basis. HCAI recognizes that this may be sensitive information regarding an individual but it is important for HCAI to know of and review this information in the beginning so it can address it promptly and to assure the public that HCAI is acting diligently to protect their personal data.

[118] Cal. Civil Code section 1786.18 [regarding the California Investigative Consumer Reporting Agencies Act].

g. Sections 97392(a)(12), 97394(a)(13), 97396(a)(14), 97398(a)(15), and 97400(a)(13), Data Security

This application requirement is similar to a CURES regulation[119] and requires the applicant to state their data security for confidential HPD data. There are different requirements based on whether the applicant will access the data through the Enclave, or if there will be "direct transmission" of confidential HPD data. There are more thorough data security requirements for "direct transmission" of confidential data as there is much more of a privacy and security risk.

i. Sections 97392(a)(12), 97394(a)(13), and 97400(a)(13)(A), Data Security for Enclave Access

These subsections are for Enclave access and require a data applicant to state their "security measures to protect against the unauthorized disclosure of confidential data" and gives examples of specific information to provide, such as the physical security for each physical location where access will take place, controls on who can view the data, and background screening for individuals who will access the data. This is related to the requirement above in which HCAI requires information about the physical location of individuals accessing data (see above regarding "List of Contractors and Individuals").

As noted above, a mandatory reason for denial is if disclosure of the confidential HPD data would "create an unreasonable risk to individual privacy or security" (per proposed section 97388(b)(3)). Having this information will allow HCAI to assess whether the data applicant will properly secure and protect confidential HPD data from being improperly released based on their circumstances.

ii. Sections 97396(a)(14), 97398(a)(15), and 97400(a)(13)(B), Data Security for "Direct Transmission" of Confidential HPD Data

These subsections are for the "direct transmission" of confidential HPD data which is more concerning than Enclave access. Unlike Enclave access, data applicants will have full control over confidential HPD data after "direct transmission" without HCAI oversight. For these reasons, HPD statute requires such data applicants to have **"**data security [that] will meet the standards that [HCAI] shall apply to personal data."[120] As discussed later regarding proposed section 97406, HCAI wishes to adopt security standards for confidential HPD data in these regulations.

These subsections require applicants to state their security plan for the confidential data and describe how they will meet HCAI's security standards in proposed section 97406. This will allow HCAI to evaluate whether the applicant can meet this statutory requirement and HCAI's security standards.

---

[119] Cal. Code Regs., title 11, section 828.6(c)(11)(A)(6) [regarding data security measures].
[120] HSC section 127673.83(c)(1) and (2).

Furthermore, a mandatory reason for denial is if disclosure of the confidential HPD data would "create an unreasonable risk to individual privacy or security" (per proposed section 97388(b)(3)). Having this information will allow HCAI to assess whether the data applicant will properly secure and protect confidential HPD data from being improperly released based on their circumstances.

HCAI requests this information from state agency applicants as well although not explicitly required by statute.[121] HCAI believes this is consistent with HPD statute's emphasis on protecting consumer and patient information and a state agency should not have lesser standards than others who obtain the same type of data since state agencies are similarly vulnerable to data breaches.[122]

h. Sections 97396(a)(15), 97398(a)(16), and 97400(a)(13)(B), Contact Information for Data Security

This is similar to the CURES regulation requirement for contact information for an entity's "information security officer."[123]

These subsections ask for the contact information for the applicant's information security officer, or as these subsections state, the individual "who will be responsible for information security of the confidential data." This is needed for applicants who have confidential data directly transmitted to them in case HCAI discovers security or privacy issues and immediate steps need to be taken by the applicant. By having this contact information, HCAI can quickly contact the person in charge of security issues instead of having to go through the individual data applicant or authorized representative.

i. Sections 97394(a)(14) and 97398(a)(17), Make Research Available to HCAI

For these types of data requests, "research identifiable data" through the Enclave and "direct transmission" of confidential HPD data, HPD statute requires that the applicant make its research using the HPD data "available to" HCAI.[124]

These subsections incorporate these statutory requirements and ask the applicant to agree to make its research available to HCAI. HCAI requires this in the application to make sure the applicant knows of this requirement and to process applications more efficiently by having applicant agree or not agree to this in the beginning.

---

[121] *See* HSC section 127673.83(d) [regarding state agency requests for confidential HPD data].
[122]For instance, the alleged theft of confidential data from the California Department of Finance in December 2022. *See* Lindsey Holden, *California investigates cybersecurity incident at Department of Finance*, The Sacramento Bee, (December 12, 2022), https://www.sacbee.com/news/politics-government/capitol-alert/article269915257.html (last accessed 1/23/2023).
[123] Cal. Code Regs., title 11, section 828.6(c)(6).
[124] HSC section 127673.83(b)(2)(D) and (c)(2).

j. Sections 97394(a)(15) and 97398(a)(18), Committee for the Protection of Human Subjects Documentation

For these types of data requests, "research identifiable data" through the Enclave and "direct transmission" of confidential HPD data, HPD statute requires that the applicant's project be "approved by the Committee for the Protection of Human Subjects [CPHS] pursuant to subdivision (t) of Section 1798.24 of the Civil Code [part of the IPA]."[125]

These subsections incorporate these statutory requirements and ask the applicant to provide documentation of CPHS approval or the applicant's plan to seek the Committee's approval during HCAI's application review or afterwards (via the conditional approval process stated in proposed section 97410). HCAI requires this in the application to determine whether the statutory requirement has been met, or whether the applicant has a suitable plan to obtain this approval (see discussion about proposed section 97410 regarding why CPHS approval is not required before applying for HPD data). These subsections also provide notice to the applicant that CPHS approval is needed for these types of requests, and makes applicant come up with a plan so that the HPD application process is not unduly delayed or held in limbo.

8. CCR, title 22, sections 97398, Unique Application Requirements for "Direct Transmission" of Confidential HPD Data

HPD statute is most protective of "direct transmission" of confidential HPD data and uniquely limits such disclosures only to "researchers."[126] For these reasons, this type of data request has unique application requirements to incorporate these statutory requirements.

a. Sections 97398(a)(3), Researcher Documentation

As noted above, this request can only be made by a "researcher" pursuant to HPD statute.[127] HCAI defined "researcher" for these regulations (as explained above). This subsection requires the applicant to submit "documentation establishing that the applicant is a researcher as defined" by these regulations. HCAI requires this to initially determine that the applicant is eligible for this type of data.

b. Sections 97398(a)(4), Organization with Which the Researcher is Affiliated

[125] HSC section 127673.83(b)(2)(B) and (c)(2).
[126] *See* HSC section 127673.83(c)(2).
[127] HSC section 127673.83(c)(2).

This is substantially similar to CURES regulation which requires a researcher to identify the entity with which the researcher is affiliated."[128] This subsection requires the same as well as identification of any entities, if any, for which the researcher desires to conduct research.

HCAI requires this information in the application to determine what parties are involved in the researcher's project to evaluate whether there may be concerns or issues that could affect the application review. For example, these data requests require approval of the HPD Data Release Committee. Knowing what entities are involved in the research will allow HCAI to identify potential conflicts of interest between a data application and Committee members.

c. Sections 97398(a)(5), Whether Researcher or Affiliated Organizations Submits Data to HPD

This subsection requires the researcher to state whether they or their affiliated organization submits data to the HPD. This will allow HCAI to more easily check whether the requester or their affiliated organization is complying with HPD statutes and regulations when determining whether to approve or deny the application under proposed section 97388(c)(2). HCAI is also required to establish a data "user fee schedule and fee waivers" for HPD data and HPD statute requires HCAI to "make considerations" regarding fees for "data submitters."[129] There may be HPD data price reductions for data submitters, and this will make it easier for HCAI to identify what data fees should be assessed if an application is approved.

This is different from similar provisions discussed above as it accounts for the researcher's affiliated organization. It is assumed that the researcher will conduct research under that affiliated organization and thus, HCAI must know whether that affiliated organization is a data submitter.

d. Section 97398(a)(12), Expertise with Privacy Protection and the Analysis of Large Sets of Confidential Information

This subsection adds to the above requirements about the requester's expertise[130] and implements an additional statutory minimum requirement[131] for "direct transmission" of confidential HPD data. Specifically, for this type of HPD data request, HPD statute also requires that the requester "has documented expertise with data security and the protection of large sets of confidential data."[132]

---

[128] Cal. Code Regs., title 11, section 828.6(c)(6).
[129] HSC section 127674(f)(2).
[130] See above regarding proposed sections 97394(a)(10), 97396(a)(11), and 97398(a)(12).
[131] *See* HSC section 127673.82(e) [stating that HCAI data release policies or regulations "shall include at least the privacy protection standards specified in Section 127673.83"].
[132] HSC section 127673.83(c)(2).

To review applications for this statutory requirement, through this subsection, HCAI will require the requesting researcher to describe their "expertise with data security and the protection of large sets of confidential data" and to provide documents in support of their expertise as statute requires "documented expertise." HCAI will review this information and determine if the requester meets this statutory requirement on a case-by-case basis.

9. CCR, title 22, sections 97392 to 97400, Unique Mandatory Reasons for Denial of HPD Data Applications

The following subsections state additional mandatory reasons for denial of data requests based on the type of HPD data request. Each data request has unique statutory requirements, and these subsections reflect these requirements that an applicant must meet to receive HPD data. These specific reasons for denial are included under each application section for the type of data request at issue so that it is clearer and easier for the public to find them and understand that they relate only to a specific data request. Although some of these unique reasons are repeated for different types of data requests, HCAI believes this presentation makes it clearer as it may overly complicate proposed section 93788, regarding "General Reasons to Deny Data Applications."

Many of these reasons for denial are incorporated into the application requirements previously discussed so HCAI has an initial basis to review these issues.

a. Section 97392(b) regarding Enclave Access to "Limited Data"

HPD statute requires that use of this data is "for research and analysis purposes consistent with program goals."[133] This subsection (b) implements this requirement and states that an additional reason for denial is if HCAI determines that the use of data is not for research or analysis purposes. This is needed to implement statute and to clearly notify requesters beforehand the reasons why their applications may be denied.

b. Section 97394(b) regarding Enclave Access to "Research Identifiable Data"

HPD statute has several additional requirements for "research identifiable data" through the Enclave. HPD statute states that this access can only be provided if the several conditions are met.[134] This subsection implements these statutory requirements and is intended to clearly notify requesters beforehand the reasons why their applications may be denied.

i. Section 97394(b)(1)

[133] HSC section 127673.83(b)(1).
[134] HSC section 127673.83(b)(2).

HPD statute requires the use of this type of data request be for "research projects."[135] This subsection implements this requirement and states that HCAI will deny a data application for this data if the use is not for a research project.

ii. Section 97394(b)(2)

HPD statute requires the use of this data be for projects "that offer significant opportunities to achieve [HPD] goals."[136] This subsection implements this requirement and states that HCAI will deny a data application for this data if the applicant's project does not meet this condition. This will be determined on a case-by-case basis.

iii. Section 97394(b)(3)

HPD statute requires that for this type of data request, the HPD Data Release Committee must have recommended "project approval."[137] This subsection implements this requirement and states that HCAI will deny a data application for this data if this Committee does not recommend project approval.

iv. Section 97394(b)(4)

HPD statute requires that for this type of data request, the Committee for the Protection of Human Subjects pursuant to Civil Code section 1798.24(t) approved the applicant's project."[138] This subsection implements this requirement and states that HCAI will deny a data application for this data if this Committee does not approve the project.

v. Section 97394(b)(5)

HPD statute requires that for this type of data request, the requester have "documented expertise with privacy protection and with the analysis of large sets of confidential data."[139] This subsection implements this requirement and states that HCAI will deny a data application for this data if the requester does not have this expertise.

As explained earlier regarding the applications requirements under sections 97394(a)(10), 97396(a)(11), and 97398(a)(12), the focus here is on an individual, the "authorized representative," having "documented expertise" instead of an organizational applicant.

vi. Section 97394(b)(6)

[135] HSC section 127673.83(b)(2).
[136] HSC section 127673.83(b)(2).
[137] HSC section 127673.83(b)(2)(A).
[138] HSC section 127673.83(b)(2)(B).
[139] HSC section 127673.83(b)(2)(C).

HPD statute requires that for this type of data request, the applicant must make its research from the confidential HPD data available to HCAI.[140] This subsection implements this requirement and states that HCAI will deny a data application for this data if the applicant does not agree to do this.

c. Section 97396(b) regarding "Direct Transmission" of "Standardized Limited Datasets"

HPD statute has several additional requirements for the "direct transmission" of "standardized limited datasets." HPD statute states that this data can only be provided if several conditions are met.[141] This subsection implements these statutory requirements and is intended to clearly notify requesters beforehand the reasons why their applications may be denied.

i. Section 97396(b)(1)

HPD statute requires that HCAI specify the purposes for each of the "standardized limited datasets" it develops.[142] For this reason, applicants must use the "standardized limited datasets" consist with these purposes to comply with HPD statute. This subsection implements this requirement and states that HCAI will deny a data application for this data if the proposed use is inconsistent with the purposes specified for the "standardized limited dataset."

ii. Section 97396(b)(2)

HPD statute requires the requester have "documented expertise with privacy protection and with the analysis of large sets of confidential data."[143] This subsection implements this requirement and states that HCAI will deny a data application for this data if the requester does not have this expertise.

As explained earlier regarding the applications requirements under sections 97394(a)(10), 97396(a)(11), and 97398(a)(12), the focus here is on an individual, the "authorized representative," having "documented expertise" instead of an organizational applicant.

iii. Section 97396(b)(3)

HPD statute requires that for this type of data request, the HPD Data Release Committee must have recommended "project approval."[144] This subsection implements this requirement and states that HCAI will deny a data application for this data if this Committee does not recommend project approval.

---

[140] HSC section 127673.83(b)(2)(D).
[141] HSC section 127673.83(c)(1).
[142] HSC section 127673.83(c)(1).
[143] HSC section 127673.83(c)(1).
[144] HSC section 127673.83(c)(1).

d. Section 97398(b) regarding "Direct Transmission" of Confidential HPD Data

HPD statute has the most additional requirements for an entity for the "direct transmission" of confidential HPD data. HPD statute states that this data can only be provided if several conditions are met.[145] This subsection implements these statutory requirements and is intended to clearly notify requesters beforehand the reasons why their applications may be denied.

i. Section 97398(b)(1)

HPD statute only allows a "researcher" to make this type of data request.[146] This subsection implements this requirement and states that HCAI will deny a data application for this data if the applicant is not a "researcher" which is defined in these regulations.

ii. Section 97398(b)(2)

HPD statute requires the use of this type of data request be for "research projects."[147] This subsection implements this requirement and states that HCAI will deny a data application for this data if the use is not for a research project.

iii. Section 97398(b)(3)

HPD statute requires the use of this data be for projects "that offer significant opportunities to achieve [HPD] goals."[148] This subsection implements this requirement and states that HCAI will deny a data application for this data if the applicant's project does not meet this condition. This will be determined on a case-by-case basis.

iv. Section 97394(b)(4)

HPD statute requires that for this type of data request, the HPD Data Release Committee must have recommended "project approval."[149] This subsection implements this requirement and states that HCAI will deny a data application for this data if this Committee does not recommend project approval.

v. Section 97398(b)(5)

HPD statute requires that for this type of data request, the Committee for the Protection of Human Subjects pursuant to Civil Code section 1798.24(t) approved the applicant's

[145] HSC section 127673.83(c)(2).
[146] HSC section 127673.83(c)(2).
[147] HSC section 127673.83(c)(2) [incorporating the requirements in HSC section 127673.83(b)(2)].
[148] HSC section 127673.83(c)(2) [incorporating the requirements in HSC section 127673.83(b)(2)].
[149] HSC section 127673.83(c)(2) [incorporating the requirements in HSC section 127673.83(b)(2)].

project."[150] This subsection implements this requirement and states that HCAI will deny a data application for this data if this Committee does not approve the project.

vi. Section 97398(b)(6)

HPD statute requires that for this type of data request, the requester have "documented expertise with privacy protection and with the analysis of large sets of confidential data"[151] and also "documented expertise with data security and the protection of large sets of confidential data."[152] This subsection implements this requirement and states that HCAI will deny a data application for this data if the requester does not have this expertise.

As explained earlier regarding the applications requirements under sections 97394(a)(10), 97396(a)(11), and 97398(a)(12), the focus here is on an individual, the "authorized representative," having "documented expertise" instead of an organizational applicant.

vii. Section 97398(b)(7)

HPD statute requires that for this type of data request, the applicant must make its research from the confidential HPD data available to HCAI.[153] This subsection implements this requirement and states that HCAI will deny a data application for this data if the applicant does not agree to do this.

e. Section 97400(b) regarding State Agency Requests for Confidential HPD Data

HPD statute has additional requirements for state agencies to receive confidential HPD data as it incorporates a statutory provision from the IPA, Civil Code section 1798.24(e), which generally allows state agencies to share personal information with other state agencies.[154] This incorporated IPA statute states that a state agency can only receive this data if some conditions are met. This subsection implements these statutory requirements and is intended to clearly notify requesters beforehand the reasons why their applications may be denied.

i. Section 97400(b)(1)

Civil Code section 1798.24(e) allows HCAI to share confidential HPD data with other state agencies if the data "transfer is necessary for the transferee agency to perform its constitutional or statutory duties." This subsection implements this requirement and

[150] HSC section 127673.83(c)(2) [incorporating the requirements in HSC section 127673.83(b)(2)].
[151] HSC section 127673.83(c)(2) [incorporating the requirements in HSC section 127673.83(b)(2)].
[152] HSC section 127673.83(b)(2).
[153] HSC section 127673.83(c)(2) [incorporating the requirements in HSC section 127673.83(b)(2)].
[154] HSC section 127673.83(d); and Cal. Civil Code section 1798.24(e).

states that HCAI will deny a data application if the state agency does not need the data for its constitutional or statutory duties.

ii. Section 97398(b)(2)

Civil Code section 1798.24(e) allows HCAI to share confidential HPD data with other state agencies if the data "use is compatible with a purpose for which the information was collected." This subsection implements this requirement and states that HCAI will deny a data application if the state agency's use is not compatible with a purpose for which HPD data was collected (which are stated in HPD statute[155]).

10. CCR, title 22, section 97402, Data Release Committee

For three types of HPD data requests (section 97394 to access "research identifiable data" in the Enclave, section 97396 for "direct transmission" of "standardized limited datasets," and section 97398 for "direct transmission" of confidential HPD data), HPD statute requires that the HPD Data Release Committee recommend approval of the data applicant's project.[156] This section, section 97402, states the procedure for this Committee to review and make recommendations on these data requests.

Subsection (a) states what types of data requests have the HPD Data Release Committee requirement. This is needed for clarity and to notify potential data applicants if this applies to their data application.

Subsection (b) states HCAI's process after receiving a data application that needs Committee review—that, HCAI will send a copy of the application to the Committee to make its recommendation. This is needed to notify data applicants how the process to obtain the Committee's recommendation will be started and that HCAI will initiate the process.

Subsection (c) states the Committee's procedure to review the data application for its recommendation on the applicant's project. The Committee is a "state body" under the Bagley-Keene Open Meeting Act[157] and must have open and public meetings in which they deliberate and take action.[158] This subsection implements this requirement and requires the Committee to review the applicant's project at one of its public meetings and states that the Committee may require the applicant to attend a meeting to present or respond to questions or issues. This is needed to give notice and clarity to data applicants on what they will be expected to do in regard to Committee review. This

[155] HSC section 127673.83(d).
[156] HSC section 127673.83(b)(2)(A), (c)(1), and (c)(2).
[157] Cal. Gov. Code sections 11120 to 11133.
[158] Cal. Gov. Code section 11121 [definition of "state body"]; Cal. Gov. Code section 11123(a) [requiring "state bodies" to have "open and public" meetings]; and *see* HSC section 127673.84(g) [noting a per diem for Committee members to attend a "data release committee meeting].

section also notes that the Committee will issue a "written recommendation" after the meeting about the applicant's project. This is to make sure that the recommendation is in writing, separate from meeting minutes, which will create a clear and distinct record of the recommendation. This will make it easier to document and notify applicants about the Committee's recommendations.

11. CCR, title 22, section 97404, Committee for the Protection of Human Subjects

For two types of HPD data requests (section 97394 to access "research identifiable data" in the Enclave, and section 97398 for "direct transmission" of confidential HPD data), HPD statute requires approval of the data applicant's project by the Committee for the Protection of Human Subjects (CPHS).[159] The CPHS is a state entity that is outside of HCAI and is currently administered by the California Health and Human Services Agency's Center for Data Insights and Innovation.[160] This section, section 97404, states HCAI's requirements to the applicant regarding CPHS review.

Subsection (a) states what types of data requests have the CPHS requirement. This is needed for clarity and to notify potential data applicants if this applies to their data application.

Subsection (b) states that HCAI will allow (1) the applicant to seek CPHS approval before or during HCAI's review of the data application, or (2) the applicant to seek review after HCAI conditionally approves the data application pursuant to a later regulatory section (section 97410) regarding conditional approvals. The purpose of this is to give flexibility and discretion to the data applicant on how they want to obtain CPHS review, since CPHS is outside of HCAI and HCAI has no control over CPHS's procedure. This is needed to make the HPD data application process more efficient for the CPHS and the applicant, and to make this process as convenient as possible without creating unnecessary roadblocks for the data applicant. For instance, a data applicant may want to make sure it gets all of HCAI's approvals before proceeding to the CPHS instead of wasting resources by first going to CPHS only to have HCAI deny the application.

Conditional data application approvals by HCAI related to CPHS review will be discussed later regarding proposed section 97410.

12. CCR, title 22, section 97406, Data Security Standards for the Direct Transmission of Confidential HPD Data

[159] HSC section 127673.83(b)(2)(A), and (c)(2).
[160] HSC section 130205(a).

As discussed above (regarding proposed section 97388(b)(6)(B)), HPD statute requires data applicants requesting "direct transmission" of confidential HPD data to have "data security" that "meet[s] the standards that the department shall apply to personal data."[161] As discussed above, HCAI chooses to apply this as well to state agencies.[162] This proposed section, section 97406, establishes the data security standards that HCAI "shall apply" to confidential HPD data.

a. Section 97406(a)

Subsection (a) of this section contains definitions regarding data security that are only applicable to this section. The purpose of this section is that there are various terms regarding data security that are repeated, and it would be cumbersome to have to continually explain terms, especially since some of the terms require significant explanation. Thus, the definitions are needed to ensure that the regulations that follow meet the clarity requirement and to provide the specificity necessary for compliance with the regulations. The following explains each term that is defined.

i. Section 97406(a)(1), "NIST"

The federal agency, the National Institute of Standards and Technology, is referenced several times. This agency is commonly referred to as its acronym, NIST, which is defined here for clarity.

ii. Section 97406(a)(2), "FIPS 140 Validation"

NIST's Federal Information Processing Standards Publication (FIPS) 140 series are security standards by the federal government that provide requirements for cryptographic modules (i.e., hardware, software, or firmware that implements data security functions[163]), which protect sensitive but unclassified information.[164] These standards are used by NIST's Cryptographic Module Validation Program to validate cryptographic modules for use by federal agencies.

This term, "FIPS 140 Validation," is defined here to mean current validation by NIST's Cryptographic Module Validation Program under the currently applicable FIPS 140, which is periodically amended and adopted by NIST because it is used several times in section 97406. HCAI believes it would be less cumbersome and clearer for this to be explained in one place than multiple times.

iii. Section 97406(a)(3), "FIPS 200"

[161] HSC section 127673.83(c)(1) and (c)(2).
[162] This is discussed above regarding proposed section 97388(b)(6)(B).
[163] This definition is from NIST, Information Technology Laboratory, Computer Security Resource Center, *Cryptographic module*, unknown date, https://csrc.nist.gov/glossary/term/Cryptographicmodule (last accessed 11/9/2022).
[164] NIST, *Federal Information Processing Standards Publication 140-2*, May 25, 2001, page iii.

This term, “FIPS 200,” is defined here for clarity as it is used several times in this section and so that it is clear that this document is being incorporated by reference in these regulations.

iv. Section 97406(a)(4), “Information System”

This term, “information system,” is used several times in this section and thus it is defined here for clarity so that its meaning is clear to data applicants. This definition is from FIPS 200, and it is used because this section utilizes FIPS 200, which is incorporated by reference into these regulations.[165]

v. Section 97406(a)(5), “NIST 800-53”

This term, “NIST 800-53,” which is defined to include two related but different NIST publications, is defined here for clarity because it would be cumbersome and confusing to include it in the regulatory requirement later on. Without this term, HCAI would have to identify the two NIST publications, which have lengthy names, in a later section while trying to clearly state what the data applicant has to do. It is clearer to have a simple term for these publications and placed in one definitions section so a potential data applicant can find it easily.

Also, through this definition, HCAI incorporates by reference the two NIST publications into these regulations. This is again done for clarity so that it is clear that HCAI is incorporating by reference these documents instead of having to state it within the regulatory requirement.

vi. Section 97406(a)(6), “NIST 800-88”

This term, “NIST 800-88,” which is defined to include a segment of a NIST publication, is defined here for clarity because it may be confusing to explain it within a regulatory requirement later on and would be cleaner to include in this definitions subsection where a data applicant can look it up easier. Also, this publication is incorporated within this definition, so it is clearer that HCAI is incorporating this publication by reference. The “NIST 800-88” and what parts of it that are incorporated by reference will be discussed later.

b. Section 97406(b)

As required by HPD statute,[166] in this subsection (b), HCAI establishes the data security standard that data applicants must meet for “direct transmission” of confidential HPD data. HCAI chose to incorporate the current data security standard utilized by the State

[165] FIPS 200, March 2006, page 7.
[166] HSC section 127673.83(c)(1) and (c)(2).

of California and federal agencies, and which is imposed by the federal Centers for Medicare and Medicaid Services (CMS) on data recipients. These standards are the following as stated in section 97406:

- "FIPS 200" or the Federal Information Processing Standards Publication 200, "Minimum Security Requirements for Federal Information and Information Systems," dated March 2006;

- 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.

The State of California, including HCAI, currently uses these standards for its information security programs per the State Administrative Manual.[167] Federal agencies are also required to comply with these standards for information security.[168] CMS also requires entities to comply with these standards when receiving CMS identifiable data.[169] HCAI executed a data use agreement[170] with CMS and currently must comply with these standards since HCAI is receiving identifiable data from CMS for the HPD (as required by HPD statute[171]).

Subsection (b) goes on to note that the minimum level of security from those standards is for "information that is categorized as moderate-impact for the security objective of confidentiality." The terms "moderate-impact" and "security objective of confidentiality" are special terms used for these federal standards. The first step in using these federal standards is to categorize the information to be protected as "low-impact," "moderate-impact," or "high-impact" for each of the three "security objectives of confidentiality, integrity, and availability" per another federal publication, Federal Information Processing Standards Publication 199, dated February 2004 (FIPS 199).[172] Based on this categorization, as discussed in FIPS 200, an entity must select appropriate security controls and baseline of security controls in the NIST 800-53 publications.[173]

For the purposes of FIPS 200 and the NIST 800-53 publications, HCAI already determined under FIPS 199 that confidential HPD data is "moderate-impact" for the "security objective of confidentiality." For purposes of HPD, the other two security objectives in FIPS 199, "integrity" and "availability", are irrelevant as HCAI is only concerned with "confidentiality," which means protecting the data from "unauthorized

[167] California State Administrative Manual, Section 5300.5, revised 12/2019.
[168] FIPS 200, page v, section 8.
[169] Centers for Medicare & Medicaid Services, *Agreement for Use of Centers for Medicare & Medicaid Services (CMS) Data Containing Individual Identifiers,* June 2010, Form CMS-R-0235, page 3, section 7.
[170] CMS Data Use Agreement No. RSCH-2020-55668, executed by HCAI on June 3, 2020.
[171] HSC section 127673.2(b) [HCAI "shall seek data on Medicare enrollees from the federal Centers for Medicare and Medicaid Services and shall incorporate that data, to the extent possible."].
[172] FIPS 200, page 4, Section 4.
[173] FIPS 200, page 4, Section 4.

disclosure."[174] "Integrity" is about "unauthorized modification or destruction of information," and "availability" is about "disruption of access to or use of the information,"[175] which may be important for the data recipient, but not as relevant to HPD statute's focus on protecting individual privacy.

HCAI also determined that the potential impact of a loss of confidentiality would be "moderate" under FIPS 199. "Moderate" means, in part, that the loss would "result in significant harm to individuals that does not involve loss of life or serious life threatening injuries."[176] It does not appear that it would be "high" because it does not appear that a data breach of confidential HPD data would "result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries." It also does not appear that it would be "low" which means "minor harm to individuals" as there seemingly would be a significant harm to an individual's privacy. As further support, currently, in its procurement contracts that involve disclosure of identifiable information to contractors, HCAI requires its contractors to follow these federal standards and categorize this data as "moderate-impact".[177]

The language in subsection (b) also notes that it establishes a floor as it states that the 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." This language was copied from the CMS data use agreement[178] and allows a data applicant to do more than it is required under these federal standards.

c. Section 97406(c)

This subsection states specific data security requirements HCAI believes are necessary to protect transmitted confidential HPD data that may not be covered as specifically by the incorporated federal standards. Many of these requirements are adapted from what HCAI currently requires of researchers who receive patient data HCAI collects outside of the HPD[179]—specifically, the requirements in HCAI's "Required Practices for Safeguarding Access to Confidential Data."[180]

i. Section 97406(c)(1)

[174] FIPS 199, page 2.
[175] FIPS 199, page 2.
[176] FIPS 199, page 2.
[177] HCAI Procurement Contract Template, Exhibit D, *Privacy and Information Security*, section G.
[178] Centers for Medicare & Medicaid Services, *Agreement for Use of Centers for Medicare & Medicaid Services (CMS) Data Containing Individual Identifiers,* June 2010, Form CMS-R-0235, page 3, section 7.
[179] This non-HPD data is collected under the Health Data and Advisory Council Consolidation Act, HSC sections 128675 to 128810; and released to researchers under the IPA, Civil Code section 1798.24(t).
[180] This document can be found at https://hcai.ca.gov/data-and-reports/request-data/data-documentation/security-requirements/#:~:text=Administrative%20Safeguards&text=Researchers%20should%20have%20proper%20vetting,than%20what%20is%20originally%20approved (last accessed 11/9/2022).

This requires applicants to conduct a thorough background check of each individual who will work with the confidential data. It requires applicants to evaluate whether the individual presents an unreasonable risk of causing a data breach, or stealing or otherwise misusing confidential information and to prohibit those individuals from working with the data if they pose such a risk. It also requires applicants to document these checks and retain these records for a period of three years after it stops using the data.

This subsection is needed to responsibly protect confidential HPD data from those who may want to steal or misuse the data, but HCAI gives discretion to the data applicant to do these checks. These checks may reveal sensitive information about individuals, which HCAI will not normally collect, and which will remain with the applicant.

This is similar to a requirement in HCAI's "Required Practices for Safeguarding Access to Confidential Data" which requires "proper vetting… for any person who has access to data." This is also a common requirement in other state agreements. The language in subsection (c)(1) is adapted from similar provisions in HCAI's procurement contracts in which contractors may have access to personal information, [181] and in agreements the California Department of Public Health uses for entities to access personal information from them.[182]

This subsection requires the applicant to document these checks and to retain those records for three years. This is so that HCAI or another state agency can audit the applicant for compliance, and also to review if something occurs. The retention period is three years because this matches state contract record retention requirements for audit.[183]

ii. Section 97406(c)(2)

For "direct transmission," HCAI will electronically transmit confidential HPD data to the data applicant if their data application is approved. For this reason, HCAI requires that all computers that will receive and contain confidential HPD data to have "full disk encryption using modules with FIPS 140 validation" to properly protect that data if those computers are stolen. By having "FIPS 140 validation" (as discussed above), HCAI has assurance that the modules are sufficient to protect the data.

This is currently required in HCAI's "Required Practices for Safeguarding Access to Confidential Data."

iii. Section 97406(c)(3)

[181] HCAI Procurement Contract Template, Exhibit D, *Privacy and Information Security*, section E.
[182] California Department of Public Health, Center for Health Statistics and Informatics, Data Application Agreement, Section 1.B, "Background Check," Form CDPH IPSR (07-19).
[183] Cal. Gov. Code section 8546.7 [regarding the State Auditor having the ability to audit state contracts three years "after final payment under the contract"].

For the same reasons as above, in case of theft or loss, this subsection requires the applicant's "removable media devices containing confidential data [to be] encrypted with software that has FIPS 140 validation."

iv. Section 97406(c)(4)

This subsection notes that the HCAI will review and approve the applicant's ability to transmit confidential HPD data outside of the applicant. This is needed so that HCAI can properly review the risks of such transmittals and deny or request changes to data applications based on that risk.

However, if the applicant is allowed to transmit the data, for the same reasons discussed above, in case of theft or other loss, this subsection requires the applicant to use software that has "FIPS 140 validation" to encrypt confidential data when being electronically transmitted outside the applicant's system.

For mailings of unencrypted confidential HPD data, such as in hardcopy form, HCAI requires the applicant to take further actions to prevent the intentional or accidental disclosure of confidential information.

v. Section 97406(c)(5)

This subsection requires that the applicant keep unencrypted confidential HPD data within its work offices and in stored areas when unattended, not viewable from the outside. This is needed to prevent those working with the data from transporting or working on it in less secure areas, which would increase the risk of data exposure or loss. Also, this lessens the risk of unauthorized data disclosure.

vi. Section 97406(c)(6)

These security requirements apply to "research identifiable data," which has the most identifiable data elements per HIPAA.[184] This subsection requires these direct personal identifiers to be segregated from other confidential data so that if one set is breached, the most sensitive information will not be disclosed. This is needed to protect this highly sensitive information and to minimize the risk of a catastrophic data breach.

vii. Section 97406(c)(7)

This subsection discusses "media sanitization" or the "process that renders access to target data on the media infeasible for a given level of effort."[185] This subsection requires that applicants sanitize hard copy and digital media with confidential data as described in a federal standard, NIST Special Publication 800-88, Revision 1 (NIST

[184] HSC section 127673.83(c)(2) [incorporating the "direct personal direct personal identifiers listed in Section 164.514(e) of Title 45 of the Code of Federal Regulations"].
[185] NIST Special Publication 800-88, Revision 1, *Guidelines for Media Sanitization,* December 2014, page iv.

800-88). HCAI requires this because this NIST standard is widely accepted, such as being used in CURES regulation[186] and in HCAI's "Required Practices for Safeguarding Access to Confidential Data" document.

HCAI only incorporates by reference section 5 and Appendix A of NIST 800-88 for this subsection (through the definition explained above) as those parts of NIST 800-88 describe the actual methods to sanitize specific media. The other parts of NIST 800-88 are not relevant for this purpose.

By having this requirement, HCAI can be more confident that an applicant is appropriately disposing of media that has confidential HPD data.

viii. Section 97406(c)(8)

This subsection requires applicants to have their devices that have confidential HPD data to have "security patches applied in a reasonable time." This is a requirement from HCAI's "Required Practices for Safeguarding Access to Confidential Data" document. This is needed so that devices with confidential information are not left vulnerable when a device is updated through security patches. This will minimize the risk of improper disclosure of confidential HPD data.

ix. Section 97406(c)(9)

This subsection requires minimum requirements for passwords used by applicants to access confidential HPD data. NIST states that password length has been found to be a primary factor in characterizing password strength. Whereas NIST requires a minimum of 8 characters, industry experts commonly state as best practice a minimum of 16 characters is the new standard.

x. Section 97406(c)(10)

This subsection requires the use of "malicious code protection mechanisms." Endpoint security technologies used by applicants must utilize technology that addresses both signature and signature-less detection and prevention techniques. This technology must detect and prevent memory-based and/or "file-less" attacks while providing real-time on-agent prevention and detection, without the need for constant remote connectivity or updates. Most modern end-point protection software utilize signature and signature-less protection. This base level requirement protects against known vulnerabilities (signature) as well as zero-day threats (signature-less).

This subsection also requires the applicant to list the products they use, and the current version of the products in their data applications for HCAI review. This is needed to

[186] Cal. Code Regs., title 11, section 828.6(g)(4) and (h) [incorporating by reference NIST Special Publication 800-88, Revision 1].

allow HCAI to determine if the applicant is utilizing appropriate mechanisms that will actually protect confidential HPD data.

d. Section 97406(d)

This subsection provides an exemption process for the data security requirements in subsection (c) if the applicant cannot meet any of the requirements because of their unique circumstances. This subsection notes that HCAI will only exempt an applicant if it has an adequate alternative. This subsection is needed so that entities are not unfairly excluded from obtaining confidential HPD data through "direct transmission" because of their unique circumstances. However, HCAI requires that the applicant have adequate alternatives. HCAI will decide this on a case-by-case basis.

HCAI also allows this for researchers who obtain non-HPD confidential data from HCAI and is stated in HCAI's "Required Practices for Safeguarding Access to Confidential Data" document.

13. CCR, title 22, section 97408, Special Requirements for Medi-Cal Information

"Medi-Cal" is the State of California's Medicaid program, a public health insurance program created under federal law, but administered by the states. HPD statute requires HCAI to collect Medi-Cal data from the California Department of Health Care Services (DHCS) for inclusion in the HPD.[187] HCAI plans to release confidential Medi-Cal data (i.e., data with identifiable or record-level information about patients or individual consumers) through the HPD Data Use, Access and Release Program. However, as Medi-Cal is a federal program, federal law has requirements that affect this.

Federal law requires the State of California to have a "single state agency to administer or to supervise" the Medi-Cal program.[188] This single state agency is DHCS in California.[189] For this reason, DHCS has final say for the State of California on decisions that affect the Medi-Cal program, including the disclosure of Medi-Cal information in the HPD.

Federal law also requires that Medi-Cal data "concerning applicants and recipients" is only used or disclosed for "purposes directly connected with… the administration of" Medi-Cal. This was incorporated into California law, which states, that Medi-Cal data

[187] HSC section 127673(c)(4).
[188] 42 U.S.C. section 1396a(a)(4) and (5); *see* DHCS, *Overview of Medi-Cal Data*, August 2018, page 22, https://www.dhcs.ca.gov/dataandstats/data/Documents/OverviewofMedi-CalData.pdf (last accessed November 11, 2022).
[189] *See* HSC section 127674(e) ["… working through the sole state agency for Medicaid, the State Department of Health Care Services…"].

"shall not be open to examination other than for purposes directly connected with the administration of the Medi-Cal program."[190] DHCS reiterates this requirement and notes that federal law "restricts DHCS from disclosing protected information other than for purposes that are directly connected with the administration of the Medi-Cal Program."[191]

Based on the above, this section, section 97408 states additional requirements and procedures if a data applicant wants Medi-Cal data from the HPD. Specifically, additional information an applicant needs to provide in its application for DHCS, that DHCS will review requests for Medi-Cal information as the State of California's single state agency, and that such requests will be denied if DHCS denies the request for Medi-Cal information.

a. Section 97408(a)

DHCS has its own process for entities to obtain Medi-Cal data including its own data application.[192] This subsection incorporates aspects from DHCS's data application that are not addressed by HPD's application requirements, so that DHCS will have the information it needs to review requests for Medi-Cal information via HPD.

i. Section 97408(a)(1)

This subsection requires the applicant in its HPD data application to specify how its data "project will benefit the Medi-Cal program." This language is copied from DHCS's data application[193] and is asked so it can be determined whether the data use will comply with the federal requirement that Medi-Cal data only be used for "purposes directly connected with… the administration of" Medi-Cal.

ii. Section 97408(a)(2)

This subsection requires the applicant to state "the funding sources for applicant's project." This language is also copied from DHCS's data application.[194] As DHCS explains in its application, this is required because:

---

[190] Cal. Welfare & Institutions Code section 14100.2(a).
[191] DHCS Website, *Application Materials for Requesting Access to Protected Data*, November 7, 2022, https://www.dhcs.ca.gov/dataandstats/data/Pages/DRCApplication.aspx (last accessed 11/10/2022).
[192] *See* DHCS Website, *Accessing DHCS Protected Data for Research and Public Health,* May 2, 2022, https://www.dhcs.ca.gov/dataandstats/data/Pages/AccessingProtectedData.aspx (last accessed 11/10/2022).
[193] DHCS, *Application to Obtain Protected DHCS Data for Research*, August 2018, section IX, https://www.dhcs.ca.gov/dataandstats/data/Documents/DRC%20Applications/DRC-New-Application-2019.pdf (last accessed 11/10/2022).
[194] DHCS, *Application to Obtain Protected DHCS Data for Research*, August 2018, section V, https://www.dhcs.ca.gov/dataandstats/data/Documents/DRC%20Applications/DRC-New-Application-2019.pdf (last accessed 11/10/2022).

> "In general, the DHCS […] will not support research that will lead to the creation of a product or tool that the researcher or funder intends to market. For example, [DHCS] may deny data requests from requestors wanting to evaluate the impact of prescription drugs if a pharmaceutical company finances the study directly or indirectly."

iii. Section 97408(a)(3)

Lastly, this subsection requires the applicant to state "whether the project will assist in the development of a commercial product." This language is also copied from DHCS's data application.[195] As discussed above, DHCS's policy is not to "support research that will lead to the creation of a product or tool that the researcher or funder intends to market." So, this requirement is to assess that issue.

b. Section 97408(b)

This subsection notes that all such requests are subject to DHCS's review (as discussed above), and states HCAI's procedure to obtain DHCS review of requests for Medi-Cal information—that it will forward a copy of applicant's complete application to DHCS for review. This is necessary to notify data applicants about the need for DHCS review and also what steps will be taken to obtain this review, so the applicant knows they do not have to take any additional steps for this.

c. Section 97408(c)

This subsection states HCAI will deny a request for Medi-Cal information in an HPD data application if DHCS denies the request. This is for the reasons discussed above—that DHCS is the single state agency for Medi-Cal and has authority over decisions regarding Medi-Cal. The purpose of this subsection is to make clear to the applicant that their request can be denied based on DHCS's review and decision.

HCAI does not state anything about DHCS's review process or how it decides this because it is a separate state agency. These regulations do not restrict or require DHCS to do anything regarding its review and DHCS may create its own processes and procedures in handling these requests.

14. CCR, title 22, section 97410, Decisions on Data Applications

HPD statute requires that HCAI "maintain information about… the disposition of requests and shall develop processes for the timely consideration and release of

[195] DHCS, *Application to Obtain Protected DHCS Data for Research*, August 2018, section XII, https://www.dhcs.ca.gov/dataandstats/data/Documents/DRC%20Applications/DRC-New-Application-2019.pdf (last accessed 11/10/2022).

nonpublic data."[196] This section, section 97410, addresses these statutory requirements and states how and when HCAI will decide on data applications that are submitted. This is needed to notify applicants of when data applications will be reviewed and how HCAI will notify applicants about decisions.

a. Section 97410(a), Decision Timelines

Subsection 97410(a) is about the timeline for decisions on HPD data applications and is a way to address the statutory requirement to have "timely consideration" of data applications.

Subsection 97410(a)(1) requires HCAI to notify applicants in writing about the decision within 60 days of complete submission of an application. HCAI believes that 60 days is a reasonable amount of time to be able to process an application since some applications may be complex especially if it is about the "direct transmission" of confidential HPD data. This subsection notes that the 60 days does not trigger until a "complete submission" of the application is made. This is required as HCAI may not be able to make a decision without all the information required under these regulations.

This subsection (a)(1) also gives HCAI a process to extend the 60-day period for good cause and provides a list of circumstances that may warrant extension. These include when the applicant agrees to a longer period, or if there are issues outside of HCAI's direct control, such as if an application requires review by a committee or DHCS.

However, subsection (a)(2) requires HCAI to notify the applicant of the extension, including the length and reasons for it. It also requires HCAI to send this notice to the applicant at least 10 days before it is supposed to issue a decision. The reason for this is so that HCAI keeps the applicant informed about its application and also to provide transparency for HCAI's actions. This will allow applicants to follow-up with HCAI as necessary and also build trust between HCAI and applicants.

b. Section 97410(b), Decision Notices

This subsection (b) is about meeting the statutory requirement to "maintain information about… the disposition of requests…." HCAI does this by requiring a written "decision notice" for HPD applications to have explanations for HCAI decisions. Specifically, when denied, subsection (b)(1) requires the written notice to have the scope of denial (in whole, or in part and what parts). This is to notify the applicant about why they were denied so they can mitigate or fix any issues and to provide transparency over HCAI's actions to build trust in the program. If approved, subsection (b)(2) requires the scope of the approval, the fee for the data as set by HCAI, how the data will be provided to the

[196] HSC section 127673.82(g).

applicant, and a copy of the data use agreements, if any, required to receive data. Data use agreements, as discussed later, are required for confidential HPD data, but may be required for other data. This subsection also requires HCAI to explain why data use agreements are required.

This subsection is needed to provide adequate information to the applicant and to create documentation about the data request as required by statute. It is to increase transparency and to establish trust in HCAI that HCAI is operating this program fairly. With this information, an applicant can also raise concerns about any decisions it finds unwarranted and may be able to correct deficiencies or other issues that prevent them from receiving HPD data.

c. Section 97410(c), Conditional Decision Notices

As mentioned above, HCAI will allow an applicant needing to get approval from the Committee for the Protection of Human Subjects (CPHS) to seek that approval after HCAI's review and conditional approval—i.e., approval of the data application except for the CPHS approval piece.[197] This subsection discusses how this is allowed and the process to follow for conditional approvals.

HCAI is establishing this conditional approval process for applications needing CPHS review based on HCAI's long history of providing confidential data to researchers outside of HPD. HCAI's experience has been that not allowing this will cause delays and waste resources. For example, if a researcher first obtains CPHS approval and then comes to HCAI to obtain data, the researcher may have to go back to CPHS if HCAI changes or requires more of the researcher's data security (which is not uncommon). This delays the process for the applicant to receive data and also wastes HCAI's and CPHS's resources. Another example is that CPHS may approve the project, but HCAI may not because of HPD requirements, which would waste resources for CPHS and the applicant. For this reason, HCAI gives the applicant the option to wait until after HCAI gives its conditional approval to go to CPHS.

This subsection states that conditional approvals are only for those data applications needing CPHS review and that HCAI may issue conditional approval before the CPHS makes a decision. This is to clearly notify the applicant what conditional approvals are for and when HCAI will issue such approvals.

Subsection (c)(1) requires, after a conditional approval is issued, the applicant to notify HCAI within 10 days after the applicant receives CPHS's decision. Whether CPHS denies or approves the application, this notification will allow HCAI to finish processing an application instead of applications being held in limbo.

Subsection (c)(2) states that HCAI will issue a final decision notice to the applicant within 30 days after receiving the CPHS's decision. It also notes that the HCAI's final

[197] *See* discussion regarding proposed section 97404 above.

decision may be different from its conditional approval. This is to cover any circumstances in which the CPHS review or decision changes HCAI's decision on the application, whether to deny or alter the approval. This also gives HCAI discretion to change the notice if it has other cause to do so. This subsection is needed to notify the applicant on the final steps of this process and to make it clear to the applicant that the final decision can change and may be different after CPHS review.

15. CCR, title 22, section 97412, Data Use Agreements for Confidential Data

HPD statute requires "each person" who receives or works with confidential HPD data to "sign a data use agreement."[198] Subsection (a)(1) implements this statutory requirement and requires that a data applicant and each individual who will work with confidential data to execute a data use agreement before accessing confidential data.

Subsection (a)(2) states that HCAI, for non-confidential HPD data, may require, for good cause, an applicant and each individual who works with the HPD data to execute a data use agreement. HPD statute's protections and emphasis is on record-level and identifiable information about patients and consumers. However, HPD data may include other sensitive information, such as personal information about individual medical providers, and proprietary contracting/pricing information. This subsection gives HCAI the discretion to impose a data use agreement in circumstances in which HCAI determines that HPD data is sensitive and needs more protection. This will be done on a case-by-case basis depending on the data and data use.

Subsection (b) states required provisions for data use agreements for those who receive confidential HPD data. This is to ensure that all data use agreements will have these requirements regardless the circumstance because of their importance.

Subsection (b)(1) requires an applicant to only use or work with confidential HPD data in the United States of America. The reasons for this requirement are discussed above.[199] This is needed for every confidential HPD data approval as the problems with confidential HPD data being observed, controlled, used or stored in other countries will not change with the type of data or use.

Subsection (b)(2) requires the data use agreement to be governed and construed under the laws of the State of California and that any court action will be litigated in the Sacramento County Superior Court. Choice of law could be uncertain if an out-of-state entity requests and receives confidential HPD data and this will make this issue clear, so the parties know what laws to apply to the agreement. HCAI is headquartered in Sacramento and thus, it is most convenient and efficient for HCAI to have any litigation based on a data use agreement be at the Sacramento County Superior Court.

[198] HSC section 127673.83(a).
[199] Discussion above regarding proposed section 97388(b)(8).

16. CCR, title 22, section 97414, Fee Reduction

HPD statute requires HCAI to "adopt regulations on […] fee waiver."[200] Section 97414 is to meet this statutory requirement and creates a partial fee waiver or fee reduction process for entities regarding the price of HPD data.

a. Section 97414(a)

Subsection (a) states that HCAI may reduce data fees on specific data applications if HCAI determines there is good cause to do so. This subsection notes that this regulation is only about fee reductions for specific data applications at issue, and that it is not establishing blanket reductions. HCAI is still determining its fee schedule for HPD data release, and the fee schedule may have different rates for different types of applicants or data uses. This regulation is not for categorical reductions, but the process to evaluate individual applications.

Subsection (a)(1) and (a)(2) give examples of "good cause" for fee reduction. Subsection (a)(1) notes that financial hardship of the applicant may be good cause for reduction. HCAI does not want to prevent an applicant from using HPD data because of a lack of financial resources. Subsection (a)(2) notes that a reduction may be made to encourage the use of HPD data in high priority areas or which could lead to innovations. This example is to cover situations in which a fee for HPD data may cause an applicant to abandon a project which HCAI determines to be important or particularly worthwhile because of its public benefit.

b. Section 97414(b)

Subsection (b) sets the process for an applicant to request a fee reduction. It requires the applicant to submit a written request for a fee reduction with their application and to include a justification for a reduction with supporting documentation. HCAI needs this at the very beginning to assess whether an application fee reduction is warranted and needs this information to make the determination whether to grant a fee reduction or not.

Subsection (b) also notes that HCAI may seek more information about their reduction requests. This is to provide notice to applicants what other actions HCAI may take regarding these requests.

c. Section 97414(c)

[200] HSC section 127674(f)(3).

This subsection (c) states HCAI's process after the fee reduction request is made to HCAI—that HCAI will notify applicants of its decision with its application decision notice, which is discussed in section 97410 above. HCAI may not be able to finally assess the data fee until after it has come to a decision on the application because the type and amount of data may change during the application review process. At the time the application decision is ready, HCAI will be able to assess the data fees and determine whether reduction is appropriate.

17. CCR, title 22, section 97416, Restrictions for Public Data Products

HPD statute requires that HCAI develop "policies and procedures" for the disclosure of aggregated and deidentified individual consumer and patient data "in a publicly available analysis, data product, or research"[201] and regarding "data aggregation and the protection of individual confidentiality, privacy, and security for individual consumers and patients."[202]

This section 97416 is to meet this statutory requirement. This section states requirements that data users, i.e., data applicants who were approved for and received confidential HPD data, must follow when creating "public data products" (defined in these regulations and discussed above).

a. Section 97416(a)

This subsection reiterates and interprets HPD statute's requirement that no record-level or identifiable information about patients and individual consumers is to be released in a "public data product."[203] It notes that data users can only include "aggregated" and "deidentified" data about patients and individual consumers in its "public data products." This is to clearly give notice to data users regarding what they can put into their "public data products" when using confidential HPD data.

Subsection (a)(1) states how data users are to deidentify confidential HPD data. This subsection requires the data user to comply with the California Health and Human Services Agency's "Data De-Identification Guidelines (DDG)," dated September 23, 2016, to deidentify confidential HPD data for use in public data products, and these guidelines are incorporated by reference here. HCAI incorporates the Guidelines as the way to deidentify data because the Guidelines were prepared by professionals by HCAI's oversight agency, the California Health and Human Services Agency, and has been used by HCAI and many other state departments to deidentify data. Only certain parts of the Guidelines are incorporated because the Guidelines has sections only applicable to state agencies and only the sections about the methodology for deidentification are relevant for the purposes of this regulation. Also, the Guidelines

[201] HSC section 127673.81(c)(2).
[202] HSC section 127673.5(b).
[203] HSC section 127673.81(a).

provides an example way of deidentification, the "Publication Scoring Criteria." This subsection makes this example mandatory for a data user when deidentifying data. HCAI is familiar with this method and by making it mandatory, will make it far easier for HCAI staff to review how a data user deidentified data (as discussed later).

b. Section 97416(b)

Subsection (b) states the process in which HCAI will review a data user's "public data products" to make sure that they have been sufficiently deidentified and aggregated before release. HCAI requires that it review the "public data products" as an additional check to make sure that no private information about consumers and patients becomes public. HCAI believes this is necessary to make sure that data users are diligent in protecting individual information and to make sure that data users are competent in doing this.

Subsection (b)(1) requires data users to submit documentation regarding how they aggregated and deidentified the confidential HPD data along with their draft "public data products." This will make it easier and more efficient for HCAI to review the "public data products" and determine whether the data user properly deidentified and aggregated the confidential data.

Subsection (b)(2) describes HCAI's actions when it finishes its review of the "public data products." The first part of this subsection informs data users that they cannot release their "public data products" unless HCAI first approved of the release in writing. This is to make it clear to the data user about when they can release their "public data products." This subsection goes on to state that if HCAI does not approve the "public data product" it will inform the data user in writing of the decision and the reasons for its decision. This writing is so that the data user can more easily fix issues that HCAI identified about the "public data product."

c. Section 97416(c)

This subsection is about identifiable or record-level data of individuals who are not patients or individual consumers. As discussed above, HPD statute only explicitly protects patient and individual consumer information[204], but the HPD may collect personal information about others, such as individual providers. These other individuals still have a constitutional right of privacy in California and HCAI does not want these individuals harmed by having their private information publicly released. For this reason, this subsection prohibits data users from disclosing this type of information if it would infringe on that individual's privacy or safety.

[204] HSC section 127673.5(a)(2); and HSC section 127673.81(a) and (b).

Subsection (c)(1) requires data users to notify HCAI if their "public data products" will include identifiable or record-level data about these other individuals and requires them to describe that data to HCAI. HCAI needs this information for purposes of subsection (c)(2).

Subsection (c)(2) states that HCAI may require its review and approval of "public data products" that has other individual data before they are publicly released. HCAI will use the information received pursuant to subsection (c)(1) to determine whether it needs to review these "public data products." HCAI will determine this on a case-by-case basis depending on the data to be publicly disclosed.

Subsection (c)(3)(A) states that data users cannot release "draft public data products" with other individual information if it is under review by HCAI and not until HCAI approved the release in writing. This is to ensure that data users do not, if HCAI is reviewing a "public data product" under this subsection, release it without HCAI approval. This is to make sure that sensitive private information is not released.

Subsection (c)(3)(B) states that if HCAI does not approve the draft "public data product" under this subsection (c), HCAI will notify the data user in writing including the reasons for its decision. This is so that HCAI clearly gives clear notice to the data user, creates a record, and is being transparent with the data user. This subsection (c)(3)(B) also notifies data users that HCAI may require the data to be aggregated or deidentified for it to be released. This is needed to inform the data user what HCAI may require them to do if a draft "public data product" is not approved.

V. ECONOMIC IMPACT ANALYSIS

The proposed regulations will only impact entities who choose to request and obtain HPD data. Therefore, economically, HCAI concludes that:

1. this regulatory action will not impact a representative private person or business;

2. this regulatory action will not create jobs within the state;

3. this regulatory action will not eliminate jobs within the state;

4. this regulatory action will not create new businesses;

5. this regulatory action will not eliminate existing businesses;

6. this regulatory action will not affect the expansion of businesses currently doing business in the state;

7. this regulatory action will not impact California business' competitiveness;

8. this regulatory action will not impact small business because the proposed regulations create a voluntary program, as such, small business are not legally required to comply with the regulations, nor to enforce the regulations, and subsequently, do not derive a benefit from the enforcement of the regulation; nor incur a detriment from the enforcement of the regulation. It is optional to request HPD data, but small businesses may be affected by the proposed regulations if they choose to request program data; and

9. this regulatory action will not directly impact housing costs;

Regarding the benefits of the HPD Data Use, Access and Release regulations to the health and welfare of California residents, worker safety, and the state's environment, a statutory purpose of the HPD is to release HPD data to members of the public and other state agencies so they can use the data to improve health care in California while properly protecting individual privacy. The Legislature hoped that by having HPD data released, members of the public would use the data to develop innovative approaches, services, and programs that may have the potential to deliver health care that is both cost effective and responsive to the needs of Californians and also would increase the transparency of health care costs and utilization. The benefit of having more comparable and useful cost transparency data is difficult to quantify as it can affect many aspects of healthcare and the economy.

VI. EVIDENCE SUPPORTING FINDING OF NO SIGNIFICANT ADVERSE ECONOMIC IMPACT OF ANY BUSINESS

The Department has determined that adoption of the proposed changes would not have an adverse economic impact on any business in the State of California because the regulations do not add any additional reporting requirements or other burdens to the existing statutorily mandated program.

VII. TECHNICAL, THEORETICAL, OR EMPIRICAL STUDY, REPORTS, OR SIMILAR DOCUMENT RELIED UPON

For such documents, please see Section IV, "Specific Purpose and Necessity of Each Proposed Regulation" section above. The documents relied upon are discussed and cited in Section IV.

VIII. CONSIDERATION OF ALTERNATIVES

No reasonable alternatives have been identified by the Department or have otherwise been identified and brought to its attention that would be more effective in carrying out the purpose for which the action is proposed, that would be as effective and less burdensome to affected private persons than the proposed action, or that would be more cost-effective to affected private persons and equally effective in implementing the statutory policy or other provision of law.