DATA USE AGREEMENT FOR NONPUBLIC PATIENT LEVEL DATA – HEALTH AND SAFETY CODE SECTION 128766

The Department of Health Care Access and Information (HCAI) is required to protect patient privacy as stated in Section 128766 of the Health and Safety Code. Any Data disclosures pursuant to this Agreement are required to be consistent with the standards and limitations applicable to limited data sets in Code of Federal Regulations, title 45, section 164.514. Any hospital or health department that receives data shall not disclose that data to any person or entity, except as required or permitted by law. In no case shall a hospital, health department, contractor, or subcontractor reidentify or attempt to reidentify any data received.

This Agreement is by and between HCAI and County of Monterey, on behalf of the *Monterey County Health Department,* hereinafter termed "Requestor."
The nonpublic patient level data provided by HCAI under this Agreement pursuant to Health and Safety Code section 128766 is described in Requestor's Limited Data Request, (Data Request), including any identified attachments, Request No. **CS0002236**, dated 10-11-2022, for the project titled "Disease Surveillance for Program Evaluation" and is hereinafter termed "Data." This Data Request is hereby incorporated by reference into this Agreement. Per this Agreement, the Requestor shall not release, share, or further distribute any Data it receives from HCAI (including any Data containing complete or partial individual patient records).

The Requestor acknowledges and agrees that the nonpublic patient level data is subject to relevant state and federal privacy and security laws with which Requestor must comply.

The parties mutually agree that HCAI retains all ownership rights to the Data, and that the Requestor does not obtain any right, title, or interest in any of the Data.

Requestor will only use or disclose the Data for the specific limited purposes and in the ways described in its approved request. Requestor is bound by all statements made in the approved request. Only those persons/entities identified in the request are permitted to access, receive, or use the Data.

As the recipient of the Data, Requestor agrees that it will:

1. Only use or disclose the Data as stated in its Data Request, or as required by law (e.g., by court order or search warrant);

    - If Requestor wants to add a use, disclosure, or persons/entities to use/receive the Data, Requestor will submit a revised Data Request stating and describing the new use/disclosure and identifying any new persons/entities to receive or use the Data;

2. Use appropriate safeguards to prevent unauthorized use or disclosure of the Data including taking measures commensurate with HCAI's "*Recommended Practices for Safeguarding Access to Confidential Data*" incorporated by reference to this Agreement;

3. Notify HCAI immediately (no later than 24 hours) of the discovery of a security breach impacting the Data, or of any use or disclosure of the Data not stated in its Data Request;

4. Be responsible for all costs incurred by HCAI (data owner) due to any security incident resulting from the Requestor's failure to perform or negligent acts of its personnel, and resulting in an unauthorized disclosure, release, access, review, or destruction, or loss,

theft, or misuse of an information asset. If the contractor experiences a loss or breach of data, the Requestor shall immediately report the loss or breach to the data owner. If the data owner determines that notice to the individuals whose data has been lost or breached is appropriate, the requestor will bear any, and all costs associated with the notice or any mitigation selected by the data owner. These costs include, but are not limited to, staff time, material costs, postage, media announcements, and other identifiable costs associated with the breach or loss of data;

5. Provide HCAI with a Business Associate Agreement that meets the requirements of the Code of Federal Regulations, title 45, Part 160 and Part 164, for any person or entity, other than a member of the Requestor's workforce, that will access PHI received by Requestor, including but not limited to Requestor's contractors, subcontractors, or partners;

6. Provide HCAI with copies of fully executed data sharing agreements, for any person or entity, other than a member of the Requestor's workforce, that will access PHI received by Requestor, including but not limited to Requestor's contractors, subcontractors, or partners. Those agreements shall reference this Agreement between the Requestor and HCAI;

7. Ensure that all of its contractors, subcontractors, or partners to whom Requestor provides any of the Data received from HCAI, agree to in writing to comply with all terms of this Agreement, including providing proof to the Requestor of destruction of the Data upon completion of the purpose specified in the approved request;

8. Not re-identify or attempt to re-identify the individuals to whom the Data pertains and not to contact any specific individual whose record is included in the Data;

9. Retain the Data for no more than ten years from the effective date of this agreement (retention period). Should Requestor need additional time beyond retention period, Requestor will need to request an extension from HCAI and provide a justification in writing. Requestor will notify HCAI within 30 days of the completion of the purpose specified in the approved request if the purpose is completed before the retention period. Within 30 days of such notice or the end of the retention period, whichever occurs sooner, Requestor, and any of its Business Associates, contractors, subcontractors, or partners must destroy the Data and send written certification of the destruction to HCAI;

    - Requestor and its Business Associates, contractors, subcontractors, or partners shall not use or retain the Data or any parts thereof, after the initial retention period or agreed upon extended retention period;

10. Present in aggregate form, in which there is no reasonable basis to believe that data can be used to identify an individual, the final report findings, listing, or publication derived from the Data in any manner (e.g., via email, website, manuscript, table, chart, study, report, etc.).

    - Requestor must follow the California Health and Human Services Agency Data De-Identification Guidelines (DDG) to determine whether aggregate data is sufficiently de-identified for reporting and may not report aggregated data if User did not follow the DDG;

Termination for Cause. Upon HCAI's knowledge of a material breach or violation of this Agreement by Requestor, HCAI may provide an opportunity for Requestor to cure the breach or end the violation and may terminate this Agreement if Requestor does not cure the breach or end the

violation within the time specified by HCAI. HCAI may terminate this Agreement immediately if Requestor has breached a material term and HCAI determines, in its sole discretion, that cure is not possible or available under the circumstances. Upon termination of this Agreement, Requestor must destroy all the Data provided under this Agreement. The provisions of this Agreement governing the privacy and security of the Data shall remain in effect until all the Data is destroyed and HCAI receives a certificate of destruction from Requestor.

Any violation of this Agreement by Requestor will be subject to appropriate legal action by the State of California. Requestor agrees to indemnify, defend, and hold harmless HCAI from any and all claims and losses accruing to any person, organization, or other legal entity resulting from its violation of this Agreement.

Requestor acknowledges that criminal penalties under the Data Practices Act (California Civil Code section 1798.56) may apply if it is determined that any person willfully requested or obtained the Data under false pretenses.

Further, the Requestor agrees that any material violations of the terms of this Agreement or any of the laws and regulations governing the use of the Data may result in permanent or temporary denial of access to HCAI data for Requestor or any of Requestor's contractors, subcontractors, partners, or other Business Associates.

The undersigned individual hereby attests that they are authorized to enter into this Agreement on behalf of that Requestor and agrees to all the terms specified herein.

Signature	*Date*
Name – Typed or Printed	*Title*
Company/Organization	*E-Mail*
Address	*Telephone number*
City, State, Zip	

Approved as to Form:

DocuSigned by:
Stacy Saetta
C0ECE1B99F444A9...

Stacy Saetta

Chief Deputy County Counsel.

4/28/2023 | 1:55 PM PDT

Approved as to Fiscal Provisions:

DocuSigned by:
Ma Mon
2617DD077D65495...

Ma Mon

Chief Deputy Auditor-Controller

4/28/2023 | 8:49 PM PDT

Click "Ctrl + P" to print this page

Limited Data Request

Request number - CS0002236

HCAI offers several types of non-public data to licensed California Hospitals and California Local Health Departments. Eligible hospitals and local health departments may request Limited Model Data Sets for Patient Discharge Data, including Inpatient (PDD), Emergency Department (EDD), and Ambulatory Surgery Center (ASD). They may also order Patient Origin/Market Share data (PO/MS), created to assist hospitals and communities facing tremendous budgetary pressures, which makes the need to understand key operating performance issues critical. In addition, there are also Prevention Quality Indicators, a set of measures that can be used with hospital inpatient discharge data to identify quality of care for "ambulatory care sensitive conditions. This is data standardized for the Agency for Healthcare Research and Quality (AHRQ PQI.)

The Limited Data Set includes Inpatient (PDD), Emergency Department (EDD) and Ambulatory Surgery (AS) files. The contents of these files, including descriptions of the variables that they contain, are described in the Non-Public Data Documentation. A cross-referenced list of variables across multiple years is contained in the Master Variable Grid.

All documentation linked on this request form can also be found on the Limited Data Request Landing Page.

§128766 of the Health and Safety Code gives HCAI the legal authority to disclose patient-level data to hospitals, Tribal Epidemiology Centers, local health departments and local health officers, and certain federal agencies conducting a statutorily authorized activity. The law provides that the disclosure be consistent with limited data set standards and limitations under 45 CFR §164.514. Any hospital that receives data under §128766 shall not disclose the data to any person or entity except as required or permitted by the HIPAA medical privacy regulations. The hospital and its contractor(s) are prohibited from re-identifying or attempting to re-identify any information received pursuant to §128766. This form must be completed if you are requesting access to a limited data set from HCAI.

Organization Identification/Eligibility

Contact Information

Health Officer: First Name

Edward

Health Officer: Last Name

Moreno

Name of Project
Disease Surveillance for Program Evaluation

Organization
Monterey County

Department:
Monterey County Health Department: Administration

Address
1270 Natividad Rad

City
Salinas

State
California

ZIP Code
93906

Health Officer Phone Number
831-755-4585

Health Officer Email Address
morenoel@co.monterey.ca.us

Additional Information
If different from above
☐ Designated Point of Contact

Purpose
Please indicate the purpose for which the data are requested
Data used for research purposes will require a Research Supplement to be attached before the form is submitted.
☒ Public Health ☐ Research

Please describe the specific limited purposes for which the data is requested
Surveillance of preventable conditions, injury surveillance, production of community assessments, and health briefs.

Please explain how the data meets the stated purpose noted above
Data are analyzed for various conditions that may not be reported on in other readily available reports or maybe age-adjusted, for which individual de-identified data are required.

Receipt and Use of Data

Data Users Within Organization

Monterey County Health Department, Planning, Evaluation and Policy Unit - Krista Hanni - Program Manager
Monterey County Health Department, Planning, Evaluation and Policy Unit - Roxann Seepersad - Epidemiologist

Will this data be released outside of the organization?
Yes

Please note, you must upload a Business Associates Agreement form or contract before submitting.
Contractors Using Data
Conduent Healthy Communities Corporation (Conduent HCC) - Norwin Espiritu - Director of Research - 100 Campus Drive, Suite 200, Florham Park, NJ 07932 - 510.314.8300 - norwin.espiritu@conduent.com - Inpatient and Emergency Department datasets for CY2014-2021.

Contractor Data Security
Conduent Healthy Communities Corporation (Conduent HCC) - All hospital utilization data will be stored on a virtual Windows Server 2016 server hosted by a HIPAA-compliant Amazon Web Service instance. - SAS v9.4 software is used to access raw data and calculate statistics from the data. - The server can only be accessed by VPN and by specific users (Conduent HCC Research Analysts and IT Staff) with permission to access the secured data. The VPN and server are password-protected. Access to the computer is logged and available in an audit trail. - Conduent Healthy Communities Corporation employees work remotely and would access the data from the privacy of their homes. Conduent HCC staff are to prevent anyone not authorized to view patient data sets from viewing their workstation. All employee workstations have password controls and automatic logouts after inactivity. - Secure data will reside on an encrypted volume attached to the virtual server. Our secure data directories of our virtual server are explicitly excluded from our cloud backup solutions. No off-site backups of the data exist, and the virtual server is not cloned. Copies of patient health datasets will NOT be kept on any portable devices such as external hard drives, USB memory sticks, phones, or laptops under any circumstances. - Data is stored electronically on an encrypted Elastic Block Storage volume. All communications between the user and server occur over encrypted channels - Norwin Espiritu, Director of Research Margaret Mysz, Research Associate Cushanta Horton, Research Associate Richard Barnatia, Research Analyst Tim McLaughlin, Senior IT Architect - They are full-time employees of the contractor. Those with a research role are responsible for coordinating, handling, or analyzing patient data sets. Researchers will deliver analysis results to Monterey County Health based on contractual agreements and scope of work. IT personnel are responsible for permitting or restricting access to the virtual server, and for maintaining the server and its software.

Requested Data and Data Products

Indicate the database(s) and/or product(s) and year(s) of data you are requesting
Please Note: *Non-patient level data products developed using Limited Data Set confidential data are also available. Although these products are not patient level data, they are not de-identified and the requester must agree to treat the information they contain as Protected Health Information (PHI).*
☒ Patient Discharge Data (PDD)

Desired PDD Data Set
A Data Justification Grid is required if you select a Custom Data Set. The Data Justification Grid can be found

here.
☒ Model Data Set (MDS) ☐ Custom Data Set

PDD Years Desired
Enter each year desired, separated by commas. No other format will be accepted.
2014,2015,2016,2017,2018,2019,2020,2021

☒ Emergency Department Data (EDD)

Desired EDD Data Set
A Data Justification Grid is required if you select a Custom Data Set. The Data Justification Grid can be found here.
☒ Model Data Set (MDS) ☐ Custom Data Set

EDD Years Desired
Enter each year desired, separated by commas. No other format will be accepted.
2014,2015,2016,2017,2018,2019,2020,2021

☒ Ambulatory Surgery Data (ASD)

Desired ASD Data Set
A Data Justification Grid is required if you select a Custom Data Set. The Data Justification Grid can be found here.
☒ Model Data Set (MDS) ☐ Custom Data Set

ASD Years Desired
Enter each year desired, separated by commas. No other format will be accepted.
2014,2015,2016,2017,2018,2019,2020,2021

☐ Additional Products (PO/MS, AHRQ)

Statewide or Geographic Subset of Data Set(s) or Products
Please select the subset of data you are requesting
☐ Statewide Data Sets ☒ Geographic Subset Data Set or Product by county(-ies) or ZIP Code(s)

Describe and explain the set of Geographic Subset Data you are requesting
spatial and residents of Monterey County, by including both types of individuals, we can assess residents'burden of disease or incidence in the County as needed, depending on the analysis question.

Desired Data Set Format(s)
Indicate the format you prefer for your Data Set
☒ SAS (PROC Format Code Included) ☐ Comma Delimited with Labels ☐ Comma Delimited

Final Products
Will the requested data be used in any of the following ways?
☒ Geographic Information System (GIS)

Describe how this data will be used in relation to GIS
Analyses may include summarizing county data by ZIP Codes, linking to a ZIP Code layer file, and presenting data on maps. OSHPD patient counts aggregated to the ZIP code level may be layered with Monterey county zip codes.

Combination/merge/coordination with other data set(s) or databases
☒ Combination/merge/coordination with other data set(s) or databases

Describe how, including a description of the data variables within other data sets or databases
OSPHD patient counts aggregated to the ZIP code level may be layered with Monterey County ZIP attributes, generally available through US Census, such as education, income, age, and gender.

Linked patient-level information
☐ Describe the method for linking patient-level data across years/datasets

What final product(s) will be developed from this project?
Please Note: *Patient-level data cannot be contained in any product that is distributed beyond the requestor.*
Community Health Assessments, health briefs, internal reports for Health Officer or Director data requests, and public-facing data reports on Monterey County Data Share Platform (powered by Conduent LLC). For data shared with the contractor (Conduent), rates will be calculated for the following causes: asthma, community-acquired pneumonia, heart failure, hypertension, COPD, dehydration, diabetes, hepatitis, hip fractures, immunization-preventable pneumonia and influenza, urinary tract infections, unintentional falls, alcohol use, substance use, intentional self-harm, and mental health. Rates for additional causes may be calculated dependent upon the benefit to Monterey County Health and its partners.

Describe how you will treat small cells to avoid identifying individuals
Our policy is to aggregate data by year, demographic strata (i.e. age groups), and /or geographic region to increase cell size. When this method is not possible or does not adequately address the small cell the data is excluded from reporting. For data utilized by the contractor, three calendar years of data will be combined to calculate values for 3-year aggregate periods at the county level–with subpopulation rates by age group, gender, and race/ethnicity–and at the ZIP code level (with no subpopulation rates). All rates will be age-adjusted, except for the age group-specific rates that will be unadjusted. Population estimates from Claritas Pop-Facts® Demographics are used for all population denominators. County rates will be suppressed and not displayed if there are fewer than 12 cases for any of the above-listed causes of hospitalizations or ER visits. Subpopulation rates and ZIP codes rates will be suppressed and not displayed if the denominator population is less than 300 or if there are fewer than 12 cases for any of the above-listed causes of hospitalizations or ER visits. Additionally, rates by race/ethnicity for indicators specific to adolescents will be suppressed if the denominator population is 20,000 or less. Case counts for any geographic level will not be displayed or provided.

Data Security
Requesting Department
See the Appendix Security Guidelines Recommended Practices for Safeguarding Access to Confidential Data. These guidelines are an example of the information needed in the security sections below. Please be very specific about the data security.

Describe the security measures under which you propose to use, maintain, and store the requested data. Address each of the main categories below.

System on which the data will reside (Standalone computer, host-based, networked, etc.)
Data will be processed on two different computers, which are both networked within Monterey County Health Department. Conduent HCC will store data virtual server hosted by HIPAA-compliant Amazon Web Services., which is only accessible by VPN and by specific user permissions over encrypted channels.

Hardware/Software (Antivirus, anti-spyware, firewall, etc.) on department systems
The County of Monterey network security currently includes Windows Defender (with automatic security updates), Splunk, and carbon Black to monitor and audit potential malicious activity on the network and Microsoft product security. Microsoft antivirus, anti-spyware, and firewall software are installed and used on Conduent's AWS server.

Access Controls (password requirements and safeguards, VPN use, WiFi use, file sharing, logs, etc.)
Access is restricted to authorized users only. The computers are password protected with a password of at least fifteen characters in length and contain at least one alphanumeric character and one symbol. Log-in as requires two-factor authentication to verify access to authorized users. Files are only shared with authorized users with appropriate access. Authorized user includes Contractor- Conduent HCC. On the contractor's end, all hospital utilization data will be stored on a virtual server hosted by HIPAA-compliant Amazon Web Services. The server can only be accessed by VPN and by specific users (Conduent HCC Research Analysts and IT Staff) with permission to access the secured data. The VPN and server are password-protected. All communications between the user and server occur over encrypted channels. Access to the computer is logged and available in an audit trail. Conduent staff can only use work-issued computers to access the server

Physical Environment (monitor position, printer location, screen saver, etc.)
For LHD, The two computers are in separate locked offices. The offices are located in a restricted, nonpublic area that can only be entered with an electronic pass and door key. Visitor access is monitored. The monitors are positioned away from the door entry and are only accessible via password for log-in entry. Monitors are locked when not in use and screen savers are automatically triggered when no activity is detected after 5 minutes. To bypass the screen savers for access a password must be entered. For Conduent HCC, access is limited only to specific users in a restricted environment, and access to the computer is logged and available in an audit trail. Conduent Healthy Communities Corporation employees who work remotely and would access the data from the privacy of their homes. Conduent HCC staff are to prevent anyone not authorized to view patient data sets from viewing their workstation. All employee workstations have password controls and automatic logouts after inactivity.

Data Storage (e.g. removable media storage, hard drive encryption, backups of data, etc.)
For LHD, Data is not stored on local hard drives. Network files are restricted to authorized users only. Data cannot be removed or downloaded from a local hard drive onto an external, removal media storage. Backups of the data are only available on a secured SQL server which is limited to authorized users only. Copies of patient health datasets will NOT be kept on any portable devices such as external hard drives, USB memory sticks, phones, or laptops under any circumstances. For the Contractor, data is stored electronically on an encrypted Elastic Block Storage volume. All communications between the user and server occur over encrypted channels. Secure data will reside on an encrypted volume attached to the virtual server. The secure data directories of our virtual server are explicitly excluded from the cloud backup solutions. No off-site backups of the data exist, and the virtual server is not cloned. Copies of patient health datasets will NOT be kept on any portable devices such as external hard drives, USB memory sticks, phones, or laptops under any circumstances.

Encryption used on data storage drives

Monterey County Policy requires that all mobile devices that store protected information are encrypted. All protected data transmission is encrypted and supported by policies/procedures. Conduent HHC requires data to be stored electronically on an encrypted Elastic Block Storage volume and for all communications between the user and server to occur over encrypted channels.

Additional Notes

Please provide any additional notes you may have

Use of the data by Conduent is only in fulfillment of the scope specific to Monterey County and no HCAI data will be used, nor informational products are developed or shared, in support of any other effort not stated in the agreement with Monterey County. Conduent HCC will not share, transmit, or distribute HCAI data files to any external organization or to any locations outside of the virtual server. After contractual agreements between Conduent HCC and Monterey County Health have been terminated, electronic copies of data will be destroyed using Eraser (https://eraser.heidi.ie/) to destroy sensitive data files. Eraser provides a number of overwriting algorithms (the full list of algorithms can be viewed here: https://eraser.heidi.ie/appendix-a-erasure-methods/). One of the 7-pass algorithms will always be used to destroy data files. Attached is the Business Agreement between Monterey County and Conduent HCC with the amendment authorizing Conduent to include additional data analytics of deidentified hospitalization, emergency room, and mental health data to the existing platform license.

Acknowledgments and Signatures

_____ **Under HIPAA, limited data sets are Personal Health Information (PHI).**

_____ **The HIPAA Medical Privacy Rule applies to all limited data sets that I receive under this application.**

_____ **I agree to protect all nonpublic data products received from HCAI, even if they do not contain patient level data, and to treat these products as PHI.**

_____ **Any data I receive pursuant to this request will be maintained in a secure environment.**

_____ **If applying for data to use within an ACE, I certify that the applicant is an ACE.**

Name of Health Officer (printed)	**Signature of Health Officer**	**Date**

HCAI Department of Health Care Access and Information
2020 West El Camino Avenue, Suite 800
Sacramento, CA 95833
hcai.ca.gov

April 4, 2023

Edward Moreno, MD
Monterey County Health Department
1270 Natividad Rd
Salinas, CA 93906

Dear Dr. Moreno:

I am writing to confirm the Department of Health Care Access and Information (HCAI) has implemented an updated Data Use Agreement (DUA) and Limited Data Request process for confidential patient level HCAI data pursuant to California Health and Safety Code Section 128766.

The HCAI Limited DUA now includes an item allowing Limited Data Requestors to only maintain access to ten individual years of HCAI data. The item also allows for requesters to request an extension to maintain access to more than ten years of HCAI data.

Before approving data requests and to implement the ten-year limitation, HCAI is requesting a Letter of Confirmation identifying the years of confidential HCAI data the County currently maintains. If the County maintains more than ten years of data, and does not wish to request an extension, they must submit a Letter of Destruction in place of the Letter of Confirmation. The required letter must be submitted with the requester's DUA. The Letter of Destruction identifies the years of confidential HCAI data the County currently maintains, the years of data for which the County has deleted, and the method of data deletion.

HCAI will require the Letter of Confirmation or Letter of Destruction, the Data Use Agreement, and the Request Form be signed by the Health Officer, in order to proceed with the Limited Data Request Process.

If you have any questions, please contact DataandReports@hcai.ca.gov.

Sincerely,

Christopher Krawczyk

Christopher Krawczyk, PhD
Chief Analytics Officer
Healthcare Analytics Branch

COUNTY OF MONTEREY
HEALTH DEPARTMENT
Elsa Mendoza Jimenez, Director of Health
Administration | Animal Services | Behavioral Health | Clinic Services
Emergency Medical Services | Environmental Health | Public Administrator/Public Guardian | Public Health

Date

Department of Health Care Access and Information (HCAI)
Attn:
Street Address
City, State, Zip Code

RE: Letter of Destruction

In respect of confidential information disclosed to County of Monterey Health Department, Administration Bureau, 1270 Natividad Road, Salinas, CA 93906; and

Regarding California Department of Health Care Access and Information (HCAI), limited data sets that would surpass the 10-year restriction as outlined in the HCAI Data Use Agreement and in accordance with *NIST Guidelines for Media Sanitation NIST Special Publication 800-88 Revision 1*, I, [**INSERT HEALTH OFFICER NAME**] to hereby confirm, that:

a) All electronic data, including inpatient (PDD), Emergency Department (EDD), and Ambulatory Surgery (AS) limited data sets provided by the California Department of Health Care Access and Information (HCAI) have been destroyed; and
b) County of Monterey, Administration Bureau, has retained no copies of said data.

Data Destruction Procedure:

All data files that would surpass the 10-year restriction as outlined in HCAI Data Use Agreement were purged from the secured network folder directly from the source server where the data was previously stored, followed by an enhanced security erase of backups of the data that would surpass the 10-year restrictions from secured SQL networks, rendering the data virtually unrecoverable.

Name of Health Officer (printed) **Signature of Health Officer** **Date**