Guidelines to Receive California Cancer Registry Data

California Department of Public Health
Center for Healthy Communities
Chronic Disease Surveillance and Research Branch
California Cancer Registry
1631 Alhambra Boulevard, Suite 200
Sacramento, CA 95816
California Cancer Registry website (https://www.ccrcal.org/)
California Department of Public Health/California Cancer Registry Home Page

Version 1.0

Table of Contents

I. Introduction

The California Cancer Registry (CCR) is a program within the California Department of Public Health (CDPH) under the Chronic Disease Surveillance and Research Branch (CDSRB). These guidelines outline the legal requirements and procedures governing the confidentiality, security, use, access, disclosure, and publication of CCR data. All individuals and institutions accessing or possessing CCR data must adhere to these guidelines and procedures. This includes, but is not limited to:

- CDPH/CDSRB staff
- Regional cancer registries
- Other state cancer registries
- Federal cancer control agencies
- Local health officers and local health jurisdiction staff
- Researchers and their affiliated personnel
- Contractors, agents, and employees handling CCR data

Additionally, individuals with a valid scientific interest, such as those engaged in demographic, epidemiological, or other health-related research, may be granted access to confidential CCR data if they meet CDPH-determined qualifications and agree in writing to maintain confidentiality. In addition to complying with these guidelines and procedures, all authorized users must also adhere to the following:

- California (CA) Health and Safety Code (HSC) Sections 100330 and 103875-103885.

- California Information Practices Act, CA Civil Code Section 1798 et seq., and CA Welfare and Institutions Code Section 10850.

- CA Code Regs., tit. 17, Section 2593.

- All other federal and state laws or regulations applicable to confidentiality, security, use, access, disclosure, and publication of CCR data.

- The Common Rule, also known as the Federal Policy for the Protection of Human Subjects (45 CFR part 46, subpart A), and the terms and conditions of approval by an institutional review board of any human subjects research using CCR data.

If these authorities conflict, the most restrictive requirement shall govern. Failure to comply with the foregoing requirements shall result in immediate termination of all agreements for and other rights to access and/or possession of CCR data, disqualification from future use, access, or disclosure of CCR data, and any and all other remedies available by law. If you have a question about the applicability or interpretation of these requirements, please contact:

Mark Damesyn, DrPH, MPH, Chief
Chronic Disease Surveillance and Research Branch
California Department of Public Health
1631 Alhambra Boulevard, Suite 200
Sacramento, CA 95816
(916) 731-2500
Mark.Damesyn@cdph.ca.gov

These guidelines and procedures supersede the following CCR documents: “Policies and Procedures for Access to and Disclosure of Confidential Data. From the California Cancer Registry (January 2014),” “Policies and Procedures for Access to and Disclosure of Confidential Data from the California Cancer Registry (version February 2008),” “Policies and Procedures for Access to and Disclosure of Confidential Data from the California Cancer Registry (version 10/2/2006),” "Policies for Access to Confidential Data: California Cancer Registry (undated)," "Procedures for Requesting Data from the California Cancer Registry (version 10/19/01)," "Procedures for Conducting Data Linkages with the California Cancer Registry (version 10/17/2001)," and "Cancer Surveillance Section, California Cancer Registry, Confidentiality Policy and Procedures (undated)."

II. Cancer Reporting in California

In response to public concerns over the need to determine the causes and cures for cancer, the California legislature passed legislation in 1985 to mandate the reporting of all diagnosed or treated cancers (excluding basal and squamous cell carcinomas of the skin) and all deaths due to cancer and the collection of that data by the CCR. CCR was fully implemented, and statewide cancer reporting began with cases diagnosed as of January 1, 1988. The operation of CCR is governed by the authorizing legislation in sections 103875 -103885 of HSC, administrative regulations, and various reporting system standards and policy memoranda available on CCR's website.

Hospitals and other cancer reporting facilities report cancer data from their medical records. Physicians and other healthcare providers report information about cancer patients who are not referred to a facility. This information is reported within six months from the date the patient is admitted to the facility or care commences for the patient. Cancer reporting facilities and health care providers are required to employ a mechanism to ensure cancer patients are informed that cancer is a designated reportable disease and that the facility or provider will report each patient with cancer to CCR.

CCR staff use advanced data management systems to integrate and verify incoming records continuously. Through the auto-consolidation of pathology and facility reports, cases are built and quality-controlled in a dynamic environment. Once these quality assurance activities are finalized and the data achieve established completeness thresholds, they are consolidated into the statewide analysis file, ensuring the dataset captures greater than 97% of cancer cases for the target period.

In addition to their regular reporting obligations, cancer reporting facilities and healthcare providers are required to grant CCR and its authorized representatives access to all records that identify cases, characteristics, treatment, and medical status of all cancer patients. CCR utilizes this authority to ensure completeness of reporting and to undertake rapid case ascertainment. To provide comprehensive data collection, CCR has established case-sharing agreements with neighboring states, including all of California's border states. These agreements facilitate the inclusion of information on California residents diagnosed or treated for cancer in other states, thereby enhancing the completeness and accuracy of the registry's data.

CCR utilizes the Surveillance, Epidemiology, and End Results Data Management System (SEER*DMS) to efficiently manage this vast amount of data. Developed by the National Cancer Institute (NCI), SEER*DMS supports all core functions of a central cancer registry, including data collection, editing, linkage, consolidation, and reporting. By employing SEER*DMS, CCR enhances data quality, consistency, and operational efficiency, aligning with national standards for cancer surveillance. CCR and its regional registries participate in the Centers for Disease Control and Prevention's (CDC) National Program of Cancer Registries (NPCR) and in the Surveillance, Epidemiology, and End Results (SEER) program of NCI. CCR is consistently recognized by the North

American Association of Central Cancer Registries (NAACCR) for meeting the highest standards of completeness and timeliness in cancer case ascertainment, as well as the completeness of data elements collected on all cancer cases.

III. Uses of CCR Data

CCR is the cornerstone of substantial cancer research, with hundreds of funded research projects and thousands of publications relying on CCR data. In addition to funded projects and publications, researchers use CCR data to analyze demographic and geographic factors that affect cancer risk, early detection of cancer, and effective treatment of cancer patients.

Pursuant to HSC Section 103885, all CCR data is confidential information. It includes information from the CCR database and information collected but not yet incorporated into it. It includes the information and the documents, files, or other records, regardless of the format or medium in which the data are recorded.

State law allows information in medical records to be provided to CCR and its authorized agents. Once information from those records has been collected for the CCR database, HSC Section 103885 is the controlling authority concerning its use. CCR is not a covered entity under the federal Health Insurance Portability and Accountability Act (HIPAA). Consequently, the confidentiality, security, use, access, disclosure, and publication of CCR data are not subject to HIPAA requirements. However, HIPAA requirements may be relevant if a research study or other activity combines or links CCR data with protected health information covered by HIPAA.

As HSC Section 103885 provides that **all** CCR data is confidential, this means that data in the CCR database is confidential, whether or not the data identifies an individual or could be used to identify one. In the context of CCR data, confidentiality is absolute, i.e., CCR data cannot be used, accessed, disclosed, or published except as specifically authorized by HSC Section 103885. The law expressly requires that CCR and its regional registries use CCR data for demographic, epidemiological, or similar health-related studies, and for determining the sources of cancer and evaluating measures designed to eliminate, alleviate, or ameliorate their effects.

HSC Section 103885 explicitly outlines the permissible uses of CCR data. These include demographic, epidemiological, and other health-related studies aimed at understanding cancer trends, identifying the sources of cancer, and evaluating public health measures designed to mitigate cancer's impact. Qualified individuals may access or obtain CCR data for these purposes, provided they meet specific qualifications and agree to maintain the confidentiality of the data. Additionally, the law allows the publication of de-identified data in reports on cancer incidence and mortality, provided the published data does not identify individual cases or sources of information and cannot be used to re-identify individual cases or sources of information.

IV. Access to CCR data

1. General Guidelines

Access to CCR data is defined as the right to examine the data. Access to CCR data is permitted only for the purposes set forth in HSC section 103885. The right to access CCR data does not include the right to copy or retain the data or to permit another person or institution to access or copy the data unless authorized by HSC section 103885 or approved by CCR. Access is granted to individuals, not institutions.

2. Access to CCR Data for Production Purposes

A. CDPH/CDSRB Employees

CDPH/CDSRB may grant access to CCR data to CDPH/CDSRB employees and contractors working under CDPH/CDSRB's authority involved in producing and analyzing CCR data, specifically for public health surveillance, epidemiology, and the identification, monitoring, assessment, or investigation of potential public health signals, disease outbreaks, or conditions of public health significance. This access is granted only to the extent necessary for fulfilling job responsibilities. Employees and contractors are required to complete CDPH/CDSRB confidentiality and security training annually and to sign the CCR Confidentiality Pledge at the time of their assignment, and to do so annually thereafter.

CCR will maintain an access list with the following information about all persons who have been granted access to CCR data: name of the person authorizing access, name, title, address, and organizational affiliation of persons granted access, dates of access (which may cover a prospective period not to exceed one year), specific purpose(s) for which the CCR data will be used, and date on which the employee completed training and signed the CCR Confidentiality Pledge.

B. Regional Registry Employees

A CCR regional registry may grant access to CCR data to registry employees involved in data collection, surveillance, analysis, and data disclosure activities. These employees must complete confidentiality and security training annually, as per CDPH/CDSRB standards, and sign the CCR Confidentiality Pledge upon assignment to the regional registry and each subsequent year. The regional registry is required to maintain an access list with the following information about employees who have been granted access to CCR data: name of the person authorizing access, name, title, address, and organizational affiliation of the employee granted access, dates of access (which may cover a prospective period not to exceed one year), specific purpose(s) for which the CCR data will be used, and date on which the employee completed training and signed the CCR Confidentiality Pledge.

3. Access to CCR Data for Research and Surveillance

Strict protocols govern access to CCR data for research and surveillance purposes, protecting the privacy, integrity, and appropriate use of sensitive health information. Below are the key requirements and definitions.

A. Definition of Research

The California Health and Human Services Agency's Committee for the Protection of Human Subjects (CalHHS/CPHS) and CDPH/CDSRB, which oversees the CCR, adhere to the definition of research outlined in Section 46.102 of the federal Common Rule (CFR Title 45, Part 46). **Research is defined as a systematic investigation designed to develop or contribute to generalizable knowledge, including activities such as research development, testing, and evaluation.** Any activity that meets this definition is considered research under this policy, regardless of whether it is formally classified as research in other contexts. For example, certain demonstration or service programs may involve research components.

For purposes of this part, ***the following activities are deemed not to be research***:

B. Public health surveillance activities, including collecting and testing information or biospecimens, are conducted, supported, requested, ordered, required, or authorized by a public health authority. Such activities are limited to those necessary to allow a public health authority to identify, monitor, assess, or investigate potential public health signals, onsets of disease outbreaks, or conditions of public health importance (including trends, signals, risk factors, patterns in diseases, or increases in injuries from using consumer products). Such activities include providing timely situational awareness and priority setting during an event or crisis that threatens public health (including natural or man-made disasters).

For more information on CPHS policies and procedures, visit the CalHHS/CPHS website at **Committee for the Protection of Human Subjects (CPHS) website: https://www.cdii.ca.gov/committees-and-advisory-groups/committee-for-the-protection-of-human-subjects-cphs/**.

C. Access through CCR or a CCR Regional Registry

CCR and the regional registries may grant access to CCR data to individuals with a valid scientific interest in the data, who are engaged in demographic, epidemiological, or other similar health-related studies, meet the qualifications established by CCR, and agree in writing to maintain confidentiality. Individuals seeking access must submit an application sufficient to justify the request to access CCR data and, if approved, sign the CCR Confidentiality Pledge. The application must be submitted to CCR or a CCR regional registry from which the individual seeks access. The application must be reviewed and approved by an authorized individual designated by CCR or the CCR regional registry. This individual must countersign the approval, and the name and title of the person

authorizing access will be recorded in the CCR access log in accordance with Health and Safety Code Section 103885(g)(7).

D. Accessing CCR Data by Research Staff

a. Institution: A Data Recipient's institution may permit access to CCR data by individuals performing specific tasks on the recipient's behalf, provided such tasks are directly related to the approved use of the data and the individuals are identified in the approved study protocol or data request application. These individuals are considered Authorized Project Personnel under the recipient's direct supervision. All Authorized Project Personnel must sign the Confidentiality Use Agreement (Attachment 4) associated with the DUA or the Confidentiality Use Agreement (Attachment 3) of the Confidentiality Agreement for the Disclosure of California Cancer Registry De-Identified Data (Researcher) before being granted access. Granting access to individuals or entities not named in the approved protocol, or transferring data files to an external environment, constitutes Secondary Data Sharing and must comply with the requirements outlined in Section VIII: Secondary Data Sharing.

b. Access by Staff at Collaborating Institutions: A Data Recipient may permit access to CCR data by staff from collaborating institutions to carry out specific assignments directly related to the approved use. If this access is provided via remote connection to the Data Recipient's secure system, the Data Recipient retains full responsibility for ensuring the external staff adheres to all security protocols.

External collaborators seeking such access must:

i. Be explicitly listed in the Data Recipient's approved CPHS protocol.
ii. Provide information sufficient to justify the request.
iii. Complete and sign Application and Confidentiality Agreement for Access to California Cancer Registry (CCR) Data

These individuals are strictly prohibited from downloading, copying, or removing data from the Data Recipient's secure environment. Any transfer of data files to the collaborating institution's own systems constitutes Secondary Data Sharing and is prohibited for datasets containing PII unless a separate DUA between CCR and the collaborating institution is executed.

V. Disclosure of CCR Data

1. General Guidelines

Disclosure of CCR data[1] is defined as being granted the right to examine the data and to create or retain a copy of the data. As stated above, disclosure and any redisclosure of CCR data is governed by the HSC section 103885, such that only data necessary for the stated purpose of the request may be disclosed, the data may be used only for the approved purpose, and further disclosure by the recipient must be approved in writing by CCR. Under an agreement with the Department of Veterans Affairs (VA), the CCR may not release information about VA cases to researchers involved in patient-contact or cohort-linkage studies, as this may reveal the identities of veterans. However, VA cases may be included in de-identified datasets for surveillance purposes or case listings used for research, provided the data remain non-identifiable. They are not linked in a manner that could compromise confidentiality.

2. Costs of Compiling CCR Data for Disclosure

CCR data disclosure requires the CCR or the regional registry to incur high costs to obtain, compile, and transmit the requested information. The recipient must cover reimbursement of these costs.

3. Format and Transmittal of CCR Data

Data will be formatted in a mutually agreed-upon file format. Files will be encrypted using strong encryption (such as the Advanced Encryption Standard) and provided via an agreed-upon Secure File Transfer Protocol (SFTP).

CCR data are transmitted in accordance with strict protocols to maintain data integrity, confidentiality, and compliance with applicable regulations. The following procedures govern the format and transmittal of CCR data to approved recipients:

A. Data Format

Data will be formatted in a mutually agreed-upon format that accounts for the study's needs and the recipient's technical capabilities. Common formats include:

- Comma-separated values (.csv)
- Tab-delimited text files (.txt)
- Statistical formats compatible with SAS, R, STATA, or SPSS (e.g., .sas7bdat, .sav)

[1] Any sharing of CCR data beyond the originally approved use or team is considered Secondary Data Sharing and must follow the conditions outlined in Section VIII.

B. Transmittal Method

CCR data are transmitted securely via the Secure File Transfer Protocol (SFTP) to a CDPH- or CCR-hosted server. The recipient is provided with a unique, time-limited login credential for secure access.

4. Confidentiality and Data Security

CCR data is classified as confidential under Health and Safety Code Section 103885(g), and this classification applies to all CCR data, regardless of whether it contains direct identifiers. Researchers are required to implement robust administrative, physical, and technical safeguards to prevent unauthorized access, use, or disclosure of the data. These safeguards must be in place for identifiable and de-identified data to ensure compliance with state law and to uphold the integrity and confidentiality of the cancer surveillance system.

5. Disclosure to Other State Cancer Registries, Federal Cancer Control Agencies, and Local Health Officers

The CCR may enter into agreements to provide confidential CCR data to other state cancer registries, federal cancer control agencies, and local health officers, provided the disclosure complies with HSC Section 103885 and it is used exclusively to determine the sources of cancer and evaluate measures designed to eliminate, alleviate, or mitigate its effects.

Before disclosing confidential information, requesting agencies must:

1. Submit a formal application to the CCR, which will review the request to determine eligibility and compliance with legal requirements.
2. Sign a Confidentiality Agreement (CA) or DUA that outlines privacy, security, and confidentiality obligations.
3. Agree in writing to maintain the confidentiality of the data and use it only for the approved purpose.
4. Demonstrate adequate safeguards to prevent unauthorized use, disclosure, or re-identification of individuals.

6. Disclosure of CCR Data for Research

A. Letter of Support for Grant Proposals:

For a Letter of Support (LOS) intended for grant proposals, the following are required:

- A copy of the study protocol or an abstract outlining the research.
- The Principal Investigator's (PI) name and credentials.
- The title of the study.

B. Application Procedure for De-Identified CCR Data[2]

De-identified CCR Data means data that excludes the following 18 Identifiers:

i. Direct Personal Identifiers

- Names
- Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Certificate/license numbers

ii. Geographic Information

- All geographic subdivisions smaller than a state, including:
  - Street address, city, county, precinct, ZIP code, and equivalent geocodes.
  - **Exception for ZIP codes**: The first three digits may be retained *only if*:
    - The geographic unit (based on the first three digits) contains >20,000 people (per Census data).
    - For units with ≤20,000 people, the first three digits must be replaced with "000."

iii. Dates and Age Data

- All elements of dates (except year) directly tied to an individual, including:
  - Birth date, admission date, discharge date, death date.
- Ages over 89 or any date elements that could indicate such ages.
  - **Exception**: Ages over 89 may be aggregated into a single category (e.g., "90 or older").

iv. Contact and Technical Identifiers

- Telephone numbers
- Fax numbers
- Email addresses
- Web URLs (Universal Resource Locators)
- Internet Protocol (IP) addresses

v. Vehicle and Device Information

- Vehicle identifiers and serial numbers (e.g., license plate numbers)
- Device identifiers and serial numbers

---

[2] These guidelines do **not** apply to requests for CCR death-related data. Any request for death-related data must follow the separate procedures and approval pathways established by the California Department of Public Health's Center for Health Statistics and Informatics (CHSI), Research and Analytics Branch (RAB), and the Vital Statistics Advisory Committee (VSAC). Please refer to the RAB's Data Applications and Dictionaries webpage or contact HIRS@cdph.ca.gov for more information.

vi. Biometric and Image Data

- Biometric identifiers (e.g., fingerprints, voice prints)
- Full-face photographs and any comparable images

vii. Financial and Account Information

- Account numbers

viii. Other Unique Identifiers

- Any other unique identifying numbers, characteristics, or codes not already listed.

Obtaining de-identified CCR data does not require review and approval by CalHHS/CPHS. The following minimum materials must be submitted to CCR:

- A completed Application for the Disclosure of Confidential California Cancer Registry Data.
- Confidentiality Agreement regarding Disclosure of California Cancer Registry De-Identified Data signed by the data recipient.
- A list of requested data items with justifications.
- In the case of researchers, documentation that the research study has been reviewed and approved by the requestor's Institutional Review Board.

C. Application Procedure for Personally Identifiable CCR Data

a. Obtaining a CalHHS/CPHS Letter of Support

The CalHHS/CPHS requires a letter of support (LOS) from the CCR, signed by the Chief of the CDSRB and the CDPH. To obtain this letter, researchers must submit:

- A draft of the CalHHS/CPHS protocol.
- A list of data items with justifications.

Please note that obtaining a LOS does not guarantee approval of the application for CCR data disclosure or the availability of cases for patient contact studies. Once the research study is funded or otherwise approved to proceed, the researcher must submit a formal application to CCR or the appropriate regional registry to request disclosure of CCR data.

b. Obtaining CalHHS/CPHS approval

All data disclosure applications requesting CCR data for research purposes must

include documentation of approval from both CalHHS/CPHS and the institutional IRB.

- Instructions for submitting an application for CalHHS/CPHS approval can be found at Committee for the Protection of Human Subjects (CPHS) website: https://www.cdii.ca.gov/committees-and-advisory-groups/committee-for-the-protection-of-human-subjects-cphs/

c. Data Use and Disclosure Agreement (DUA)

Before obtaining CCR data, researchers must enter into a Data Use and Disclosure Agreement (DUA) with CCR. This agreement outlines the privacy and security requirements that the researcher, referred to as the "Recipient," must adhere to. The DUA governs all aspects of data use, including scope, confidentiality, data security, and conditions for sharing data with other entities.

d. List of Required Documents

The following minimum materials must be submitted to the CCR or the regional registries:

1. Submit a partially executed California Department of Public Health – California Cancer Registry Data Use and Disclosure Agreement (Research).
2. A completed Application for the Disclosure of Confidential California Cancer Registry Data.
3. Copy of protocol application approved by CPHS.
4. Both Institutional and CalHHS/CPHS IRB approval letters.
5. Grant award notice, if applicable.

If the application is submitted to a CCR regional registry, the regional registry will review the application and forward a recommendation to CCR. Approval by the Chief of CDSRB, CDPH, is required. Upon approval, CCR will fully execute a Data Use Agreement, a legal document that creates substantial ongoing obligations on the recipient regarding confidentiality, security, use, access, disclosure, and publication of CCR data, including additional obligations not specified in these guidelines.

e. Special Requirements for Research Studies Involving Patient Contact

Researchers conducting projects involving patient contact must be sensitive to the physical and emotional challenges patients may face. Although some patients may initially be disturbed to learn that their cancer diagnosis is known to others, most patients welcome the opportunity that their data will be used for research to fight cancer. In addition to the requirements set forth above and in the Data Use and Disclosure Agreement, researchers requesting disclosure of CCR data for studies that involve patient contact must comply with the following

requirements:

1. To prevent patients from experiencing undue distress that may affect their health, the CCR discourages multiple researchers from contacting cancer patients within a short timeframe, particularly during the first year post-diagnosis, when patients typically undergo treatment. Accordingly, once a patient's information has been released for a patient contact study, CCR does not release the patient's information for another patient contact study for a period of 2 years. This approach ensures that research inquiries do not overburden patients during critical treatment and recovery.

2. No patient contact is allowed for six weeks after diagnosis to give the appropriate attending physician time to inform the patient of their diagnosis and possible treatment. Exceptions to this policy, such as for Early Case Ascertainment (ECA)[3] /Rapid Case Ascertainment (RCA)[4] studies may be considered under specific circumstances. Researchers must submit a formal request to the CCR and obtain approval, providing a detailed rationale, evidence of urgency, documentation of patient protections, and relevant IRB approvals. All exceptions will be evaluated on a case-by-case basis to ensure ethical compliance and patient safety. Researchers must submit a formal request to the CCR and obtain approval, providing:

    - A detailed rationale explaining why early patient contact is necessary and justified.
    - Evidence that the study fulfills an urgent public health or scientific need that cannot be delayed.
    - A clear description of patient protections, including steps to minimize distress and ensure informed consent.
    - Relevant IRB approvals and evidence of expedited review, if applicable.
    - A comprehensive data security and confidentiality plan outlining safeguards for patient information.

3. The first contact with a patient must be in writing. Specifically, the investigator must send a contact letter explaining how the patient's name was obtained and why the CCR was created. A copy of the CCR brochure, *Cancer Research in California* (available at https://www.ccrcal.org/learn-about-ccr/about-cancer-registries/), should also be included.

4. During the patient recruitment phase of a study, any problems that arise with individual patients, for example, hostile refusals, must be promptly reported to CCR or the regional registry. Any patient who states that they do not wish to be contacted again by any researcher must be reported to the CCR or the regional

[3] Early Case Ascertainment (ECA): A methodology for systematically identifying cancer cases to study epidemiologic patterns and public health impacts.
[4] Rapid Case Ascertainment (RCA): An expedited process for identifying cancer cases shortly after diagnosis, often for time-sensitive research such as clinical trials or urgent epidemiologic investigations.

registry. This fact will be recorded in the CCR database with a “Do Not Contact” flag.

5. The researcher must notify the CCR or the regional registry liaison if they become aware of errors or omissions in the CCR data, including more current information on a patient's vital status or current address.

6. Submitting patient names to a third party (e.g., an external website) for updated follow-up is considered redisclosure and is prohibited.

7. The researcher must submit a patient contact outcome report to CCR or the regional registry within 24 months of receipt of the list of patient names.

8. The researcher may not re-contact study subjects for reasons other than as stated in the approved study.

f. Annual Reporting to CCR Regarding CCR Data Disclosure

The researcher is required to submit any renewal approval letter(s) from their institutional review board and CalHHS/CPHS, along with a current list of individuals who have access to the CCR data. If the study is complete, the researcher is required to complete the CCR Data Destruction Acknowledgement Form.

7. Compliance and Oversight

Data recipients are subject to ongoing oversight by CCR to ensure compliance with the DUA, CA, and applicable laws. CDPH/CDSRB reserves the right to audit the researcher's facilities, systems, and practices to verify adherence to data security and privacy standards. A breach of the DUA or CA may result in immediate termination of the agreement and potential legal consequences.

VI. Publications, Reports, and Statistical Compilations

1. General Guidelines

HSC section 103885 requires that reports and statistical compilations containing CCR data not identify individual cases or individual sources of information in any way and not disclose personal information about an individual that identifies or could identify an individual. The CCR and regional registry staff may release publications and make presentations to the public that contain aggregate data and conclusions drawn from studying CCR data, including journal articles, summary reports, special analyses, studies, and other documents, as well as presentations to professional organizations, the news media, and the general public. These publications may contain case counts, rates, and survival analyses derived from CCR incidence and mortality data. Individual cases or individual sources of information shall not be identified in any way. Publications of data by the CCR and designated Regional Registries shall meet the requirements of the CDPH Data De-Identification Guidelines. Refer to the link embedded here: CDPH Data De-Identification Guidelines for a PDF version of the CDPH Data De-Identification Guidelines.

Recipients of CCR data may release publications and make presentations to the public that contain aggregate data and conclusions drawn from studying CCR data, including journal articles, summary reports, special analyses, studies, and other documents, as well as presentations to professional organizations, the news media, and the general public. These publications may contain case counts, rates, and survival analyses derived from CCR incidence and mortality data. Individual cases or individual sources of information shall not be identified in any way. Publications of data shall adhere to de-identification standards that are at least as stringent as the CDPH Data De-Identification Guidelines. Researchers shall provide an electronic or paper copy of any journal article from their research using the CCR data to the Chief of the CDSRB, CDPH.

2. Acknowledgement and Disclaimer

All publications shall contain the CCR's most current acknowledgment and disclaimer. A current acknowledgment and disclaimer can be found on the California Cancer Registry Submit Data page.

VII. Non-Availability of CCR Data for Subpoena or Other Compelled Production

HSC Section 103885 protects CCR data from compelled production. To effectuate the statutory immunity, no person or institution in possession of CCR data shall grant access to, disclose, admit, produce, or otherwise make available any part of the CCR data in any civil, criminal, administrative, or other tribunal or court proceeding, whether voluntarily or under compulsion. The person or institution shall immediately notify CDPH/CDSRB by telephone and fax of the receipt of a subpoena, discovery request, court order, search warrant, or other form of compulsory legal process, or any threat of compulsory legal process, in which CCR data and/or documents, data files, or other materials containing CCR data are sought to be produced or examined. The person or institution to whom a subpoena or order is directed for the production of or access to CCR data shall immediately notify CCR and take all necessary legal action to oppose and resist any such compulsory legal process, e.g., file a motion to quash or written objections to a subpoena or file written objections to a discovery request and opposition to a motion to compel.

VIII. Secondary Data Sharing

Pursuant to Health and Safety Code section 103885, all CCR data are confidential and may be used only for the approved research purpose. Secondary data sharing is permitted only in accordance with the California Cancer Registry Data Disclosure Guidelines for Secondary Data Sharing. The originally approved Recipient remains responsible for ensuring that any secondary sharing complies with these requirements. The following conditions apply:

1. De-Identification Requirement

Secondary sharing of CCR data is permitted only if the data are de-identified and anonymized. All CCR data disclosed to third parties must be de-identified in accordance with the Health Insurance Portability and Accountability Act Safe Harbor method, which excludes the eighteen identifiers described in 45 CFR 164.514(b)(2)(i). When CCR data are linked with external sources, the entire linked dataset must be de-identified before any secondary disclosure.

2. Direction and Control of Secondary Sharing

All secondary sharing must occur under the direction and control of the originally approved Recipient, who remains responsible for data security and confidentiality, and for ensuring that secondary sharing complies with CCR policy. Secondary recipients must use the data only for legitimate scientific or public health purposes and may not attempt to identify or reidentify any individual.

3. Conditions for Sharing De-Identified Data

De-identified CCR data may be shared through:

Controlled access repositories that review access requests, control and audit dataset access, and require data use agreements prohibiting further sharing and requiring destruction of data upon project completion; or other investigator-initiated methods of sharing de-identified data, provided that a data use agreement is in place, prohibiting further sharing and requiring confidentiality and destruction of data upon project completion.

4. Minimum Necessary Standard and Data Transformations

Recipients must apply the minimum necessary standard when preparing data for secondary sharing. Recipients should determine whether suppression, aggregation, or other transformations are necessary to mitigate the risk of reidentification, in accordance with the CDPH Data De-Identification Guidelines.

5. Restrictions on Vital Statistics Data

Vital statistics data (including data from birth or death certificates) may not be redisclosed without prior approval from the CDPH Vital Statistics Branch.

6. CCR Does Not Track Secondary Sharing

CCR does not track secondary data sharing. Recipients are responsible for maintaining internal documentation sufficient to demonstrate compliance with CCR requirements; however, they are not required to submit routine reports about secondary sharing to CCR.

7. Confidentiality Obligations

All secondary recipients must agree in writing to maintain the confidentiality of CCR data and to use the de-identified data only for the approved scientific or public health purpose. Secondary recipients are prohibited from redisclosing the data except as permitted by their data use agreement.