Policies and Procedures for Access to and Disclosure of Confidential Data From the California Cancer Registry

January 2014

California Cancer Registry
Chronic Disease Surveillance and Research Branch
1631 Alhambra Boulevard, Suite 200
Sacramento, CA 95816

Version 05.2

Table of Contents

I. Introduction

The California Cancer Registry (CCR) is a program of the State of California, Department of Public Health (CDPH), Chronic Disease Surveillance and Research Branch (CDSRB). The purpose of these policies is to establish standards for, and to govern, the confidentiality, security, use, access, disclosure and publication of CCR data. All persons and institutions that have access to or possess CCR data are required to comply with the applicable provisions of these policies and procedures with respect to such data. Persons and institutions covered by these policies and procedures include CDPH, the regional registries, other states' cancer registries, federal cancer control agencies, local health officers, research institutions, and their employees, agents and contractors. In addition to these policies and procedures, the aforementioned persons and institutions are required to comply with the following (for detailed description of California codes visit http://www.ccrcal.org/Cancer_Reporting/Reporting_Legislation_and_Regulation.shtml):

- CA Health and Safety Code (HSC) Section 100330 and 103875-103885, including without limitation the provisions relating to confidentiality, security, use, access, disclosure and publication of CCR data.

- California Information Practices Act, CA Civil Code Section 1798.24 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.

The terms and conditions of any agreement entered into with CDPH/CDSRB, a regional registry, or a recipient of CCR data that relates to the confidentiality, security, use, access, disclosure or publication of CCR data. The standard agreement forms in the appendices incorporate the policies and procedures set forth herein by reference.

If these authorities conflict, the most restrictive requirement shall govern. Failure to comply with the foregoing requirements shall result in immediate termination of all 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 provided by law. If you have a question about the applicability or interpretation of these requirements, please contact:

Kurt Snipes, Ph.D., Chief
Chronic Disease Surveillance and Research Branch
California Department of Public Health
1631 Alhambra Boulevard, Suite 200
Sacramento, CA 95816
(916) 731-2500
kurt.snipes@cdph.ca.gov

These policies and procedures supersede the following previous CCR statements of policy: “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)," "Cancer Surveillance Section, California Cancer Registry, Confidentiality Policy and Procedures (undated)."

The CDPH/CDSRB has other policy documents topically related to confidentiality, security, use, access, disclosure and publication of CCR data. See the “CDPH HAM Information Security Policy, Sec. 6-1000, revised August 2009.”

These policies and procedures are updated periodically. The most current version is posted on the California Cancer Registry web site (www.ccrcal.org). Permission to reproduce these policies and procedures is hereby granted.

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. 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, and 100330 of the California Health and Safety Code, administrative regulations and various reporting system standards and policy memoranda available on CCR's website (Reporting Legislation and Regulation).

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

CCR staff ensures all information is accurate before data aggregation occurs. Once quality control activities are performed and the data are complete, they are integrated into a statewide data set. Under the current procedures, the CCR requires approximately eighteen months after the close of a calendar year to collect, verify and consolidate data to produce analysis files. These files include greater than 95% of cancer cases for a given year.

In addition to their regular reporting obligations, cancer reporting facilities and health care providers are required to grant CDPH/CDSRB and authorized representatives access to all records that would identify cases, characteristics, treatment, and medical status of all cancer patients. The CCR utilizes this authority to assure completeness of reporting and to undertake rapid case ascertainment.

Information is collected about the patient, the tumor, the treating physician, the treating facility, and the first course of treatment - over 200 data elements for each tumor. CCR also has out-of-state case sharing agreements with other states, including all of California's bordering states in order to capture information on tumors diagnosed in other states for California residents.

All of California participates 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 the National Cancer Institute (NCI). The CCR is consistently recognized by the North American Association of Central Cancer Registries for meeting the highest levels of completeness and timeliness of cancer case ascertainment and completeness of data elements collected on all cancer cases.

III. Uses of CCR Data

CCR is the cornerstone for a substantial amount of cancer research with hundreds of funded research projects and thousands of publications that have relied 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.

CCR data is defined as information collected pursuant to HSC Section 103885 and predecessor statutes. It includes information in the CCR database and information that has been collected but not yet incorporated into the database. It includes the information itself and the documents, files, or other records, regardless of format or medium in which the data are recorded.

State law allows information in medical records to be provided to CDPH and its authorized agents. Once information from those records has been collected for the CCR database, HSC Section 103885 is the controlling authority with respect to its use.

The 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. 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.

HSC Section 103885 provides that all CCR data are confidential. CDPH interprets this to mean that data in the CCR database are confidential whether or not they identify an individual or could be used to identify an individual. 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 CDPH and the regional registries use the CCR data for surveillance, cancer control initiatives and research into the causes and cures of cancer.

The law allows access to CCR data by certain qualified persons, and the disclosure of CCR data to qualified institutions for cancer control, surveillance and research. In addition, it allows the publication of reports about the incidence of and mortality from cancer, case counts and rates for specific population subgroups and local communities. Each of these permissive uses of CCR data is discussed in detail below.

IV. Access to CCR data

1. General guidelines

Access to CCR data is defined as the right to examine the data. The right to examine CCR data does not include the right to copy or retain the data or to permit another person or institution to examine or copy the data. Access to CCR data may be granted by CDPH/CDSRB or a regional registry. 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 employees assigned to the production of CCR data to the extent necessary to perform their job responsibilities. They are required to complete CDPH confidentiality and security training annually and sign the CCR Confidentiality Pledge at the time of their assignment to the CCR and annually thereafter.

CDPH/CDSRB will maintain an accessee 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. Regional registries may grant access to CCR data to persons on the CDPH/CDSRB accessee list.

b. Regional registry employees

The regional registry may grant access to CCR data to employees of the institution in which the regional registry is located who are assigned production of CCR data at the regional registry to the extent necessary to perform their job responsibilities. They are required to complete confidentiality and security training annually that meets CDPH requirements and sign the CCR Confidentiality Pledge at the time of their assignment to the regional registry and annually thereafter.

The regional registry is required to maintain an accessee 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. CDPH/CDSRB may grant access to CCR data to persons on the regional registry

accessee list.

3. Access to CCR data for surveillance and research

a. Access through CDPH/CDSRB or a regional registry

CDPH/CDSRB and the regional registries may grant access to CCR data to persons who have a valid scientific interest in the data, are engaged in demographic, epidemiological, or other similar studies related to health, meet qualifications established by CDPH/CDSRB, and agree in writing to maintain confidentiality.

Individuals seeking access must provide information sufficient to justify the request as described in the Confidentiality Agreement for Access to CCR Data (Appendix 2). In addition, they must indicate their agreement to maintain confidentiality by signing the agreement.

The Confidentiality Agreement for Access to CCR Data is a legal document that creates substantial ongoing obligations on the part of the signatory with respect to confidentiality, security, use, access, disclosure, and publication of CCR data. Individuals signing this document agree to comply in all respects with the terms and conditions of this agreement.

The signed agreement must be submitted to CDPH/CDSRB or the regional registry from which the individual seeks access. CDPH/CDSRB or the regional registry must review the request, determine that the applicant is qualified, and approve the agreement in writing prior to granting access to the individual.

CDPH/CDSRB and the regional registries will include individuals granted access to CCR data under this subsection on their accessee list.

b. Access through an institutional recipient

An institution to which CCR has disclosed data (see Section V) may grant access to the Principal Investigator who signed the Confidentiality Agreement for Disclosure of CCR Data (Appendix 3) pursuant to which the recipient institution received the data. No additional confidentiality agreement needs to be signed by the principal investigator.

Recipient institutions may grant access to CCR data to other persons to carry out a specific assignment on behalf of the institutional recipient, which is directly related to the use for which disclosure was granted to the recipient. Persons seeking access must provide information sufficient to justify the request. The individual must sign the Confidentiality Agreement for Access to CCR Data (Appendix 2).

Recipient institutions that grant access to CCR data to persons other than their principal investigator must maintain an accessee list with the following information: name of the person authorizing access, name, title, address, and organizational affiliation of the persons granted access, dates of access (which may cover a prospective period not to

exceed one year), and the specific purpose for which the CCR data will be used. A copy of the list must be provided annually to CDPH/CDSRB or the regional registry that disclosed the CCR data to the institution.

V. Disclosure of CCR Data

1. General guidelines

Disclosure of CCR data is defined as the granting of the right to examine the data and to create or retain a copy for the use of the institution. CCR data may be disclosed to an institution by CDPH/CDSRB, or a regional registry. Only data necessary for the stated purpose of the request may be disclosed. The data may be used only for the approved purpose. Further disclosure by the institution must be approved by CDPH/CDSRB (see section 6e). Under an agreement with the Veterans Administration (VA), the CCR may not release information about VA cases to researchers.

Disclosure must be requested by an individual (usually a principal investigator) and the institution with which the principal investigator is affiliated. As part of the request, the Principal Investigator and an authorized representative of the institution must meet all the requirements described in Section V.6.c. If the request is approved, the disclosure will be transmitted to the principal investigator as described in Section 3 below.

2. Costs of compiling CCR data for disclosure

Disclosures of CCR data require CDPH/CDSRB or the regional registry to incur significant costs to obtain, compile and transmit the information. These costs must be covered by the recipient institution. Contact CDPH/CDSRB or the regional registry for additional information.

3. Format and transmittal of data

Data will be formatted in a mutually agreed upon file format. Files will be encrypted using a strong encryption (such as the Advanced Encryption Standard) and emailed to the Principal Investigator using CDPH approved secure email system. If the file is too large to send via email, the file will be placed on CD ROM's and shipped overnight to the Principal Investigator via a company that is bonded and provides tracking information on the shipment, i.e. FEDEX or Golden State Overnight.

4. Data storage and security of CCR data

CCR data, defined as all documents, files or other records, regardless of format or medium, must have appropriate protections to ensure that only authorized individuals have access to the data. CCR data that are not in use should be stored in locked cabinets or rooms. Computers that store CCR data or can access the data need to be protected with a strong frequently changed password and must not be accessible from the Internet. Computers need be properly maintained with current security patches and antivirus software. If the data will be stored on a desktop, laptop, mobile computing device or other portable electronic medium the data must be encrypted and physically secured when not in use. Data shall not be left unattended in automobiles, airports, hotels or other

higher risk areas. If data are being transported then they must be encrypted and with either an authorized staff member or a secure, traceable, bonded courier. If data are being transmitted then it must be done over a secure encrypted medium. When CCR data or copies of CCR data are no longer required, they must be securely shredded or wiped from all systems and media.

5. Disclosure to other state cancer registries, federal cancer control agencies and local health officers

CDPH/CDSRB and the regional registries may enter into agreements to provide CCR data to other states' cancer registries, federal cancer control agencies and local health departments if the disclosure is for the purposes of public health surveillance. The requesting agency must indicate their agreement to maintain confidentiality of CCR data.

The request should be submitted to the CDPH/CDSRB or the regional registry from which the individual seeks data. CDPH/CDSRB or the regional registry should review the information provided to determine whether the requesting agency is eligible to receive CCR data under this subsection and whether the purpose of the request is consistent with the requirements of this subsection. If the CDPH/CDSRB or the regional registry makes a favorable determination, the request should be submitted to the Chief of CDSRB, CDPH. CDPH/CDSRB or the regional registry will disclose the data upon receipt of written approval from the Chief of CDSRB, CDPH.

6. Disclosure to research institutions

In addition to the general requirements for disclosure described in subsection 1. above, a researcher is required to demonstrate that their research has scientific merit, institutional IRB approval and documentation of approval by the California Committee for Protection of Human Subjects (CPHS).

a. Letter of support

It is strongly recommended that researchers considering studies which would utilize CCR data begin by contacting CDPH/CDSRB or a regional registry to discuss their proposed research study. If the proposed study appears to be feasible, the researcher should request a letter of support for inclusion in funding agency applications, dissertation proposals, etc. To obtain a letter of support, researchers will need to submit an abstract of the project along with the project title, and name and mailing address of the PI to CDPH/CDSRB. A letter of support does not guarantee that an application for disclosure will be approved or that cases will be available for patient contact studies. If the proposed research study is funded or otherwise cleared to proceed, the researcher should submit an application to CDPH/CDSRB or the regional registry from which disclosure is requested.

b. Obtaining CPHS approval

All data disclosure applications require documentation of approval by the California Committee for the Protection of Human Subjects (CPHS) in addition to an institutional IRB approval.

- Instructions for submitting an application for CPHS approval can be found at http://www.oshpd.ca.gov/Boards/CPHS/index.html

- CPHS Contact:
  Phone: (916) 326-3660
  E-mail CPHS at cphs-mail@oshpd.ca.gov

- The CPHS requires a letter of support from the CCR, signed by the Chief of CDSRB, CDPH. To obtain this letter, researchers will need to submit an abstract of the project along with the project title, and name and mailing address of the PI to CDPH/CDSRB and staff will provide a signed CPHS Appendix VII (letter of support) for the CPHS review process.

c. Application procedure

The following minimum materials must be submitted to CDPH/CDSRB or the regional registries for data disclosures:

1. A study protocol of the project (excluding Appendices).
2. Documentation of peer review for scientific merit. Usually, a funding agency award or dissertation committee approval meets this condition. In some cases this condition may be met by convening a regional registry or CDPH review committee.
3. Documentation that the research study has been reviewed and approved by the requestor's Institutional Review Board and CPHS.
4. Confidentiality Agreement for Disclosure of CCR Data (Appendix 3) signed by the principal investigator and an authorized representative of the recipient institution.
5. A list of requested data items with justifications (for minimum data security inclusion requirements see section 6g).

CDPH/CDSRB or the regional registry from which disclosure is requested will review the application materials and additional information may be requested. If the application was submitted to a regional registry, they will review the application and forward a recommendation to CDPH/CDSRB. Approval by the Chief of CDSRB, CDPH is required. The principal investigator will be notified in writing.

The Confidentiality Agreement for Disclosure of CCR Data is a legal document that creates substantial ongoing obligations on the part of the individual signatory in the recipient Institution with respect to confidentiality, security, use, access, disclosure, and

publication of CCR data, including additional obligations not specified in these policiesand procedures. Individuals signing this document, agree to comply, in all respects with the terms and conditions of this agreement.

d. Special requirements for research studies involving patient contact

Researchers conducting projects that involve patient contact need to be sensitive to the physical and emotional difficulties which patients may be experiencing. Although some patients initially may be disturbed to learn that their cancer diagnosis is known to individuals other than their own care-takers, most patients welcome the opportunity that their data will be used for research to fight cancer.

In addition to the requirements set forth in subsection 1 above and in the Confidentiality Agreement for Disclosure of CCR Data, researchers requesting disclosure of CCR data for studies that involve patient contact must comply with the following requirements:

1. The general policy of CCR is that multiple researchers should not contact cancer patients within a short time of each other, especially during the first year after diagnosis while undergoing therapy. In order to effectuate this policy, researchers should request the Patient Contact Availability Form from each of the regional registries (Cancer Registry of Greater California, Los Angeles Cancer Surveillance Program, and Greater Bay Area SEER registries) in whose territory each patient to be contacted resides, he or she should ensure that the patient is not included in any currently funded studies.

The CCR can only limit multiple patient contacts by researchers using CCR data. Patients may also have been contacted by researchers who received contact information from another source.

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.

3. The first contact with a patient must be in writing. Specifically, the investigator must send a contact letter to the patient that explains how the patient's name was obtained and why the CCR was created. A copy of the CCR brochure, *Cancer Research in California (*http://www.ccrcal.org/pdf/Reports/research.pdf) 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 CDPH/CDSRB or the regional registry. Any patient who states that he/she does not wish to be contacted again by any researcher must be reported to CDPH/CDSRB or regional registry promptly in writing. This fact will be recorded in the regional and statewide databases with a Do Not Contact flag.

5. The researcher must notify CDPH/CDSRB or the regional registry liaison if he or she becomes aware of errors or omissions in the CCR data and any more current information

on a patient's vital statistics and current address.

6. Submission of patient names to an external website for updated follow up is considered redisclosure and is prohibited.

7. The researcher must return the names and contact information of all patients received from CCR who were not included as subjects for the study to CDPH/CDSRB or the regional registry liaison within six months of receipt of the initial list of names. The reason for non-inclusion, e.g. decline to participate, unable to locate, physician advised no contact, should be specified for each patient.

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

e. Re-disclosure of CCR data by researchers

If the Recipient Institution has a legitimate justification for sharing CCR data with another institution, for example as part of a collaborative research project, the second Recipient Institution must obtain approval for this re-disclosure of the CCR data from the Chief of CDSRB, CDPH. The second institution must comply with all requirements of Section 6c above. Submission of patient names to an external website for updated follow up is prohibited.

f. Access to CCR data by research staff

The Recipient Institution may grant access to the CCR data to other persons to carry out a specific assignment on behalf of the Recipient Institution, which is directly related to the use for which disclosure was granted. Persons seeking access must provide information sufficient to justify the request and must sign the Confidentiality Agreement for Access to CCR Data (Appendix 2) to maintain the confidentiality of the data. A copy of the list must be provided annually to CDPH/CDSRB or the regional registry that disclosed the CCR data to the institution.

g. Annual Reporting to CCR regarding CCR data disclosure

The Recipient Institution is required to submit the renewal approval letter from the institutional IRB and CPHS IRB. The Recipient Institution is also required to submit a current list of individuals who have access to the CCR data. If the study is complete, then the Recipient Institution is required to complete the CCR Data Destruction Acknowledgement Form documenting CCR data have been destroyed.

VI. Publications, Reports and Statistical Compilations

1. General guidelines

Health and Safety Code § 103885 requires that reports and statistical compilations that contain CCR data not identify individual cases or individual sources of information in any way.

CDPH/CDSRB and regional registry staff may release publications and make presentations to the public containing aggregate data and conclusions drawn from studying CCR data, including journal articles, summary reports, special analyses, studies and other documents, and presentations to professional organizations, the news media and the 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. For example, for a geographic area with a small population (less than 10,000) the minimum number of incident cases reported for a specific anatomic site of cancer by five-year age group and race shall be five.

Recipients of CCR data may release publications and make presentations to the public containing aggregate data and conclusions drawn from studying CCR data, including journal articles, summary reports, special analyses, studies and other documents, and presentations to professional organizations, the news media and the 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. For example, for a geographic area with a small population (less than 10,000) the minimum number of incident cases reported for a specific anatomic site of cancer by five-year age group and race shall be five. Researchers are required to provide an electronic or paper copy of any journal article arising out of their research to the CCR data custodian and the Chief of the CDSRB, CDPH.

2. Acknowledgement and Disclaimer

All publications shall contain the most current acknowledgment and disclaimer. A current acknowledgement and disclaimer can be found at http://www.ccrcal.org/Data_and_Statistics/Acknowledgement&Disclaimer.shtml

VII. Procedures for Processing Patient Requests for Access to Data

Individuals have the right to access records containing their personal information maintained by CCR according to CA Health and Safety Code Section 103885 (g) (10) and the California Information Practices Act, Civil Code Sections 1798 – 1798.78. "Personal information" is information that identifies or describes an individual including his or her name, home address, home telephone number, social security number, and physical description, education, or medical or employment history.

Patients should complete the California Cancer Registry Patient Record Request Form (Appendix 5) and copy of identification and address verification. For more detailed information, please refer to Appendix 6: Patient Record Request Checklist.

In the case of a guardian or conservator who is submitting the request on behalf of the patient, an individual should complete the California Cancer Registry Patient Record Request Form (Appendix 5) and a legal document establishing the legal authority, a copy of identification, and address verification. For more detailed information, please refer to Appendix 6: Patient Record Request Checklist.

In the case of an individual requesting a deceased patient's records, an individual should complete the California Cancer Registry Patient Record Request Form (Appendix 5), a certified copy of the death certificate, and a legal document establishing the legal authority, a copy of identification, and address verification. For more detailed information, please refer to Appendix 6: Patient Record Request Checklist.

VIII. Availability of CCR Data for Subpoena or Other Compelled Production

HSC Section 100330 protects CCR data from compelled production. In order 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 shall immediately 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.

IX. Definitions

CCR data: All information collected at any time under the authority of California Health and Safety Code §10385 and predecessor statutes, whether or not such information identifies an individual or could be used to identify an individual. CCR data also means all documents, files or other records, regardless of format or medium, containing CCR data (whether alone or in combination with other data).

Access to data: The right to examine data.

Disclosure of data: The granting of the right to examine data and the right to create and retain a copy.

CCR Data custodian: CDPH/CDSRB or a designated regional registry.

Research: The same definition as 45 CFR § 46.112 (d).
http://www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.htm#46.102

Public Health Surveillance: The systematic collection, analysis, and interpretation of outcome-specific data for use in planning, implementation and evaluation of public health practice.

Aggregate data: Statistical information derived from CCR data that does not include any individual item of data representing a person, whether identified, identifiable or anonymous, and from which no information about an identifiable or anonymous person can be obtained in any manner.

Reports and statistical information: Reports, articles, special analyses, studies, and other publications and communications that contain aggregate CCR data.

Sources of information: hospitals and other facilities or agencies providing diagnostic or treatment services to patients with cancer, and physicians, surgeons, dentists, podiatrists, and all other health care practitioners diagnosing or providing treatment for cancer patients, that have provided information contained in CCR data files.

Appendix 1: California Health and Safety Code Section 103875-103885

103875. (a) The department shall conduct a program of epidemiological assessments of the incidence of cancer. The program shall encompass all areas of the state for which cancer incidence data are available. The program shall include the monitoring of cancers associated with suspected carcinogens encountered by the general public both in occupational locations and in the environment generally.

(b) The program shall be under the direction of the director, who may enter into contracts as are necessary for the conduct of the program and may accept, on behalf of the state, grants of public or private funds for the program. The director shall analyze available incidence data and prepare reports and perform studies as necessary to identify cancer hazards to the public health and their remedies.

(c) It is the intent of the Legislature that an appropriation be included in each Budget Act in an amount sufficient to provide for the annual cost of the program.

103885. (a) The director shall establish a statewide system for the collection of information determining the incidence of cancer, using population-based cancer registries modeled after the Cancer Surveillance Program of Orange County. As of the effective date of this section the director shall begin phasing in the statewide cancer reporting system. By July 1, 1988, all county or regional registries shall be implemented or initiated. By July 1, 1990, the statewide cancer reporting system shall be fully operational. Within 60 days of the effective date of this section, the director shall submit an implementation and funding schedule to the Legislature.

(b) The department may designate any demographic parts of the state as regional cancer incidence reporting areas and may establish regional cancer registries, with the responsibility and authority to carry out the intent of this section in designated areas. Designated regional registries shall provide, on a timely basis, cancer incidence data as designated by the state department to the department. The department may contract with an agency, including, but not limited to, a health systems agency, single county health department, multicounty health department grouping, or nonprofit professional association, representing a designated cancer reporting region for the purposes of collecting and collating cancer incidence data.

(c) The director shall designate cancer as a disease required to be reported in the state or any demographic parts of the state in which cancer information is collected under this section. All cancers diagnosed or treated in the reporting area shall thereafter be reported to the representative of the department authorized to compile the cancer data, or any individual, agency, or organization designated to cooperate with that representative.

(d) (1) Any hospital or other facility providing therapy to cancer patients within an area designated as a cancer reporting area shall report each case of cancer to the department or the authorized representative of the department in a format prescribed by the department. If the hospital or other facility fails to report in a format prescribed by the department, the department's authorized representative may access the information from the hospital or the facility and report it in the appropriate format. In these cases, the hospital or other health facility shall reimburse the state department or the authorized representative for its cost to access and report the information.

(2) Any physician and surgeon, dentist, podiatrist, or other health care practitioner diagnosing or providing treatment for cancer patients shall report each cancer case to the department or the authorized representative of the department except for those cases directly referred to a treatment facility or those previously admitted to a treatment facility for diagnosis or treatment of that instance of cancer.

(e) Any hospital or other facility that is required to reimburse the department or its authorized representative for the cost to access and report the information pursuant to subdivision (d) shall provide payment to the department or its authorized representative within 60 days of the date this payment is demanded. In the event any hospital or other facility fails to make the payment to the department or its authorized representative within 60 days of the date the payment is demanded, the department or its authorized representative may, at its discretion, assess a late fee not to exceed 11/2 percent per month of the outstanding balance. Further, in the event that the department or its authorized representative takes a legal action to recover its costs and any associated fees, and the department or its authorized representative receives a judgment in its favor, the hospital or other facility shall also reimburse the department or its authorized representative for any additional costs it incurred to pursue the legal action. Late fees and payments made to the department by hospitals or other facilities pursuant to this subdivision shall be considered as reimbursements of the additional costs incurred by the department.

(f) All physicians and surgeons, hospitals, outpatient clinics, nursing homes and all other facilities, individuals or agencies providing diagnostic or treatment services to patients with cancer shall grant to the department or the authorized representative access to all records that would identify cases of cancer or would establish characteristics of the cancer, treatment of the cancer, or medical status of any identified cancer patient. Willful failure to grant access to those records shall be punishable by a fine of up to five hundred dollars ($500) each day access is refused. Any fines collected pursuant to this subdivision shall be deposited in the General Fund.

(g) (1) Except as otherwise provided in this section, all information collected pursuant to this section shall be confidential. For purposes of this section, this information shall be referred to as "confidential information."

(2) The department and any regional cancer registry designated by the department shall use the information to determine the sources of malignant neoplasms and evaluate measures designed to eliminate, alleviate, or ameliorate their effect.

(3) Persons with a valid scientific interest who are engaged in demographic, epidemiological, or other similar studies related to health who meet qualifications as determined by the department, and who agree, in writing, to maintain confidentiality, may be authorized access to confidential information.

(4) The department and any regional cancer registry designated by the department may enter into agreements to furnish confidential information to other states' cancer registries, federal cancer control agencies, local health officers, or health researchers for the purposes of determining the sources of cancer and evaluating measures designed to eliminate, alleviate, or ameliorate their effect. Before confidential information is disclosed to those agencies, officers, researchers, or out-of-state registries, the requesting entity shall agree in writing to maintain the confidentiality of the information, and in the case of researchers, shall also do both of the following:

(A) Obtain approval of their committee for the protection of human subjects established in accordance with Part 46 (commencing with Section 46.101) of Title 45 of the Code of Federal Regulations.

(B) Provide documentation to the department that demonstrates to the department's satisfaction that the entity has established the procedures and ability to maintain the confidentiality of the information.

(5) Notwithstanding any other provision of law, any disclosure authorized by this section shall include only the information necessary for the stated purpose of the requested disclosure, used for the approved purpose, and not be further disclosed.

(6) The furnishing of confidential information to the department or its authorized representative in accordance with this section shall not expose any person, agency, or entity furnishing information to liability, and shall not be considered a waiver of any privilege or a violation of a confidential relationship.

(7) The department shall maintain an accurate record of all persons who are given access to confidential information. The record shall include: the name of the person authorizing access; name, title, address, and organizational affiliation of persons given access; dates of access; and the specific purpose for which information is to be used. The record of access shall be open to public inspection during normal operating hours of the department.

(8) Notwithstanding any other provision of law, no part of the confidential information shall be available for subpoena, nor shall it be disclosed, discoverable, or compelled to be produced in any civil, criminal, administrative, or other proceeding, nor shall this information be deemed admissible as evidence in any civil, criminal, administrative, or other tribunal or court for any reason.

(9) Nothing in this subdivision shall prohibit the publication by the department of reports and statistical compilations that do not in any way identify individual cases or individual sources of information.

(10) Notwithstanding the restrictions in this subdivision, the individual to whom the information pertains shall have access to his or her own information in accordance with Chapter 1 (commencing with Section 1798) of Title 1.8 of the Civil Code.

(h) For the purpose of this section, "cancer" means either of the following:

(1) All malignant neoplasms, regardless of the tissue of origin, including malignant lymphoma, Hodgkin’s disease, and leukemia, but excluding basal cell and squamous cell carcinoma of the skin.

(2) All primary intracranial and central nervous system (CNS) tumors occurring in the following sites, irrespective of histologic type: brain, meninges, spinal cord, caudae equina, cranial nerves and other parts of the CNS, pituitary gland, pineal gland, and craniopharyngeal duct.

(i) Nothing in this section shall preempt the authority of facilities or individuals providing diagnostic or treatment services to patients with cancer to maintain their own facility-based cancer registries.

(j) It is the intent of the Legislature that the department, in establishing a system pursuant to this section, maximizes the use of available federal funds.

Appendix 2: Confidentiality Agreement for Access to CCR Data

Name of applicant: _____

Title: _____

Organizational affiliation: _____

Street address: _____

City/state/zip code: _____

Instructions
Access to California Cancer Registry (CCR) data (i.e., the right to examine CCR data) is strictly limited under California law. Persons seeking access to CCR data in the custody of the California Department of Public Health, Chronic Disease Surveillance and Research Branch, or a regional registry (hereinafter the "CCR Data Custodian") must complete this application, sign and submit it to the custodian
of the data. Attach additional pages as necessary. Approval will be mailed to Applicant at the address shown above.

1. Applicant requires access to CCR data to engage in the following demographic, epidemiological or other similar studies related to health:

   _____

   _____

   _____

2. The specific purpose for which Applicant will use CCR data and the data files to be accessed (e.g. type(s) of cancer, patient characteristics, diagnosis years, geographical areas) and other relevant information are:

   _____

   _____

   _____

3. Applicant's qualifications to engage in these activities are as follows:

   _____

   _____

   _____

4. In consideration for CCR Data Custodian's approval of this application, Applicant represents, warrants, and agrees as follows:

   a. For purposes of this confidentiality agreement, "CCR data" means all information relating to cases of cancer collected at any time by the California Department of Public Health, a regional cancer registry designated by the Department or any other individual or institution under the authority of California Health and Safety Code Section 103885 and predecessor statutes, whether or not such information identifies an individual or could be used to identify an individual. CCR data also means all documents, files or other records, regardless of format or medium, containing CCR data (whether alone or in combination with other data).

   b. California Health and Safety Code Section 103885 contains various provisions relating to use, access, disclosure, and publication of CCR data. These provisions may be different from the laws, regulations or policies applicable to other data used by Applicant. Applicant represents and warrants that: (a) Applicant has reviewed section 103885, the California Department of Public Health, Chronic Disease Surveillance and Research Branch, "Policies and Procedures for Access to and Disclosure of Confidential Data from the California Cancer Registry" (www.ccrcal.org) (hereinafter "CCR Data Access and Disclosure Policies"), and the terms and conditions of this confidentiality agreement; (b) Applicant has had a full opportunity to discuss any questions or concerns Applicant may have regarding the interpretation of section 103885, Applicant's duties and obligations under the statute and the terms and conditions of this confidentiality agreement with Custodian; (c) any such questions or concerns have been resolved to Applicant's satisfaction; and (d) on the basis of the foregoing review and discussions, Applicant is prepared to access and use CCR data in conformity with section 103885 and the terms and conditions of this confidentiality agreement.

   c. Applicant agrees to comply with the requirements of California Health and Safety Code section 103885, any and all other federal and state laws or regulations relating to confidentiality, security, use, access, and disclosure of CCR data, and the CCR Data Access and Disclosure Policies.

   d. Applicant agrees to access and use the requested CCR data in strict conformity with the specific purposes set forth in his or her application. Applicant agrees not to use the CCR data for any other purpose. Applicant agrees not to copy or reproduce the CCR data in whole or in part, in any manner or format, or permit others to do so.

   e. Applicant may describe the results of Applicant's use of CCR data in professional journals, public reports, presentations, press releases and other publications, provided that a copy is provided to the institution from which Applicant receives access and that all publications contain the acknowledgment and disclaimer set forth in section VI.4. of the CCR Data Access and Disclosure Policies.

f. If Applicant becomes aware that any person or institution not authorized to access CCR data has attempted to gain access or gained access to the CCR data, Applicant agrees to immediately notify CCR Data Custodian. If Applicant inadvertently gains access to CCR data for which he or she has not been approved, Applicant agrees not to make use of the data, not disclose the data to any other person or institution, to notify the CCR data custodian, and take immediate steps to prevent any recurrence.

g. CCR Data Custodian reserves the right to withdraw Applicant's right to access and use CCR data at any time without cause. Upon receipt of notice thereof, Applicant agrees to immediately terminate its access to and use of CCR data.

h. Applicant acknowledges that if he or she fails to comply with any of Applicant's obligations under this confidentiality agreement, CCR Data Custodian and the State of California will suffer immediate, irreparable harm for which monetary damages will not be adequate. Applicant agrees that, in addition to any other remedies provided at law or in equity, CCR Data Custodian and the State of California shall be entitled to injunctive relief to enforce the provisions of this agreement.

i. Notwithstanding any other provision of this confidentiality agreement, CCR Data Custodian shall have no obligation to grant Applicant access to CCR data unless and until his or her application is approved.

By my signature I declare as follows:

I have read the foregoing agreement. By signing below I make the agreements and representations contained therein. I understand that these are material representations of fact upon which reliance was placed when this transaction was entered into.

_____
Signature

_____ _____
Printed Name and Title Dated

APPROVAL BY CCR DATA CUSTODIAN:

_____ _____
Signature Dated

_____
Printed Name and Title

Appendix 3: Confidentiality Agreement for Disclosure of CCR Data

The California Cancer Registry is a repository of cancer incidence data collected by the California Department of Public Health and regional cancer registries throughout the state of California from cancer reporting facilities and health-care providers under the authority of California Health and Safety Code section 103885. CCR data files contain medical and other personal information about identified individuals. By law, CCR data are confidential, and cannot be disclosed except in accordance with strict safeguards.

The_____("Recipient Institution")
(Name of institutional recipient)

has applied to CDSRB/California Cancer Registry ("CCR Data Custodian")
(Name of CCR Data Custodian)

for a copy of certain specified CCR data to be disclosed to

_____(hereinafter "Principal Investigator")
(Name of Primary individual recipient)

for the following proposed use:_____.
(Brief description or reference to application)

In consideration for the CCR Data Custodian's disclosure of CCR data to Principal Investigator, Recipient Institution and Principal Investigator represent, warrant, and agree as follows:

1. For the purposes of this Confidentiality Agreement:

   "Recipient Institution" is defined as the unit of government, institution, agency, the corporation, or other entity that has requested CCR data, any other unit of government, institution, agency, corporation or other entity that owns or controls the recipient institution or of which the recipient institution is a constituent part, and the directors, officers, employees, consultants, volunteers, students, contractors, agents and associates of the recipient institution.

   "Principal Investigator" is defined as the individual that the recipient institution designated in its request to receive CCR data from the CCR, and who is principally responsible for undertaking the proposed use.

   "CCR data" is defined as all information relating to cases of cancer collected at any time by the California Department of Public Health, a regional cancer registry designated by the Department or any other individual or institution under the authority of California Health and Safety Code Section 103885 and predecessor statutes, whether or not such information identifies an individual or could be used to identify an individual. CCR data also means all documents, files or other records, regardless of format or medium, containing CCR data (whether alone or

in combination with other data).

"Access to data " is defined as the granting of the right to examine data.

"Disclosure of data" is defined as the granting of the right to examine data and the right to create or retain a copy.

"Research" is defined as the same definition as 45 CFR Section 46.102(d).

"Aggregate data" is defined as statistical information derived from CCR data that does not include any individual item of data that represents a person, whether identified, identifiable or anonymous, and from which no information about an identifiable or anonymous person can be obtained in any manner.

"Reports and statistical information" is defined as reports, articles, special analyses, studies, and other publications and communications that contain aggregate CCR data.

"Sources of information" is defined as hospitals and other facilities or agencies providing diagnostic or treatment services to patients with cancer, and physicians, surgeons, dentists, podiatrists, and all other health care practitioners diagnosing or providing treatment for cancer patients, that have provided information contained in CCR data files.

2. California Health and Safety Code Section 103885 contains various provisions relating to use, access, disclosure, and publication of CCR data. These provisions may be different from the laws, regulations or policies applicable to other data used by Recipient Institution and Principal Investigator. Recipient Institution certifies that: (a) they have reviewed section 103885, the California Department of Public Health, Chronic Disease Surveillance and Research Branch, "Policies and Procedures for Access to and Disclosure of Confidential Data from the California Cancer Registry" (www.ccrcal.org) (hereinafter "CCR Data Access and Disclosure Policies"), and the terms and conditions of this confidentiality agreement; (b) they have had a full opportunity to discuss any questions or concerns they may have regarding the interpretation of section 103885 and their duties and obligations under the statute and the terms and conditions of this confidentiality agreement with the CCR; (c) any such questions or concerns have been resolved to their satisfaction; and (d) on the basis of the foregoing review and discussions, they are prepared to receive and use CCR data in conformity with section 103885 and the terms and conditions of this confidentiality agreement.

3. Recipient Institution agrees to comply with the requirements of California Health and Safety Code section 103885, any and all other federal and state laws or regulations relating to confidentiality, security, use, access, and disclosure of CCR data, and the CCR Data Access and Disclosure Policies.

4. Recipient Institution certifies that the CCR data they have requested is necessary for the above-referenced proposed use. If Recipient Institution receives CCR data that are not necessary for the above-referenced proposed use, they will immediately

notify CCR and destroy the unneeded CCR data.

5. Recipient Institution agrees to use the requested CCR data in strict conformity with the proposed use set forth above. Recipient Institution agrees not to use the CCR data for any other purpose, or for any purpose other than determining the sources of cancer and evaluating measures designed to eliminate, alleviate, or ameliorate their effect, and they agree not to permit the CCR data to be used for any other purpose. Recipient Institution agrees to notify the CCR Data Custodian and the Chief, Chronic Disease Surveillance and Research Branch, California Department of Public Health if he or she becomes aware of errors or omissions in the CCR data, or of patient vital statistics or address information that is more current than the CCR data provided to them under this agreement.

6. The Principal Investigator and members of his/her research team with a need to know may have access to the CCR data. The Recipient Institution may grant access to the CCR data to other persons to carry out a specific assignment on behalf of the Recipient Institution, which is directly related to the use for which disclosure was granted. Persons seeking access must provide information sufficient to justify the request. The individual must sign an agreement to maintain the confidentiality of the data. Recipient Institution may use the CCR's Agreement for Access to CCR Data form (available at www.ccrcal.org) or a comparable agreement for this purpose. Recipient Institution must maintain a list with the following information: name of the person authorizing access, name, title, address, and organizational affiliation of the persons granted access, dates of access (which may cover a prospective period not to exceed one year), and the specific purpose for which the CCR data will be used. A copy of the list must be provided annually to the CCR Data Custodian. Except as provided in this paragraph, Recipient Institution agrees not to grant access to the CCR data to any person, nor shall it permit persons to whom it has granted access to authorize others to have access to the CCR data.

7. Except as expressly authorized by paragraph 9 of this Confidentiality Agreement, Recipient Institution agrees not to disclose any part of the CCR data, whether or not it explicitly or implicitly identifies individuals, to any person or institution, not to copy or reproduce the CCR data in whole or in part (except as an institutional program of backup for disaster recovery or as a necessary condition of the research project), in any format or medium, and not to permit others to disclose or reproduce the CCR data. If Recipient Institution has a legitimate justification for sharing CCR data with another institution, e.g. as part of a collaborative research project, the Recipient Institution must obtain approval for this re-disclosure of the CCR data from the Chief, Chronic Disease Surveillance and Research Branch, California Department of Public Health.

8. Recipient Institution agrees to destroy all files, documents or other records containing CCR data in their custody at the earliest opportunity consistent with the conduct of the proposed use unless there is a health or research justification for retention or retention required by law. Notwithstanding the foregoing, Recipient Institution and Principal Investigator agree to destroy all files, documents or other records containing CCR data in their custody no later than three years after the date of

receipt unless the CCR Data Custodian, in its sole discretion, extends the deadline for destruction by written notice to Recipient Institution and Principal Investigator. Destruction means physical destruction of files, documents or other records, and de-identification shall not be considered destruction. Immediately following the destruction of CCR data, Recipient Institution agree to provide the CCR Data Custodian with a written declaration, executed by an authorized representative of Recipient Institution, stating that the CCR data have been destroyed.

9. Recipient Institution and Principal Investigator may include aggregate data, conclusions drawn from studying CCR data, and case counts derived from CCR data such as incidence and mortality counts (provided that such case counts do not in any way identify individual cases or sources of information) in professional journals, public reports, presentations, press releases and other publications. A copy shall be provided to the CCR Data Custodian and all publications shall contain the acknowledgement and disclaimer set forth in section VI.4. of the CCR Data Access and Disclosure Policies, and a copy shall be provided to the CCR Data Custodian and the Chief, Chronic Disease Surveillance and Research Branch, California Department of Public Health.

10. Pursuant of the California Health and Safety Code section 103885, Recipient Institution and Principal Investigator shall not 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. Recipient Institution and Principal Investigator shall immediately notify the CCR Data Custodian and the Chief, Chronic Disease Surveillance and Research Branch, California Department of Public Health by telephone and fax of the receipt of any subpoena, discovery request, court order, search warrant or other form of compulsory legal process or 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. Recipient Institution shall immediately 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.

11. If the proposed use is for research, Recipient Institution certifies that it has obtained approval for the proposed use from the Recipient Institution's committee for the protection of human subjects established in accordance with part 46 (commencing with section 46.101) of title 45 of the Code of Federal Regulations, and that they will carry out the proposed use in accordance with such approval, except that the terms and conditions of this confidentiality agreement shall take precedence. Principal Investigator agrees to provide documentation of initial IRB approval and any renewals. If the proposed research involves patient contact based on information received from CCR, the Recipient Institution agrees to follow the special requirements required by CCR for patient contact studies including approval for the proposed use from the California Committee for Protection of Human Subjects (Section V. 6. c. Policies and Procedures).

12. Recipient Institution represents that it has policies and procedures in effect

consistent with the California Information Practices Act (California Civil Code Section 1798.24 and California Welfare and Institutions Code Section 10850) to maintain the security of the CCR data in its custody, including preventing unauthorized access, and further represents that it will maintain and enforce such policies and procedures at all times during which Recipient Institution has custody of CCR data.

13. Recipient Institution certifies that it has policies and procedures in effect to implement and enforce its duties and obligations under this confidentiality agreement, and further certifies that it will maintain and enforce such policies and procedures at all times during which it has custody of CCR data.

14. If Recipient Institution becomes aware of or reasonably suspect that any provision of this agreement has been violated, or that any circumstances exist which would prevent it from complying with its obligations under this agreement, it agrees to immediately notify the CCR and take immediate steps to rectify the problem and prevent any recurrence.

15. This agreement creates a non-transferable limited license for Recipient Institution to use selected CCR data provided to them. Neither Recipient Institution nor Principal Investigator shall acquire any ownership, title or other interest in any CCR data or any copy of CCR data provided to them.

16. Recipient Institution agrees to indemnify, defend and hold harmless the State of California and the CCR Data Custodian and their respective agencies, officers, directors, employees and agents from and against any and all claims, losses, damages, costs, expenses or other liability, including attorney fees, arising out of Recipient Institution's receipt of CCR data.

17. The CCR Data Custodian reserves the right to terminate Recipient Institution's custody of CCR data by written notice at any time without cause. Upon receipt of such notice, Recipient Institution shall immediately and permanently destroy all copies of CCR data in its custody.

18. Recipient Institution acknowledges that if it fails to comply with any of their obligations under this confidentiality agreement, the CCR Data Custodian and the State of California may suffer immediate, irreparable harm for which monetary damages may not be adequate. Recipient Institution agrees that, in addition to any other remedies provided at law or in equity, the CCR Data Custodian and/or the State of California shall be entitled to seek injunctive relief to enforce the provisions of this agreement.

19. This is the entire agreement between the parties. It supersedes all prior oral or written agreements or understandings and it may be amended only in writing. This agreement, and the rights created hereunder, are individual and not assignable or otherwise transferable by Recipient Institution or Principal Investigator. This agreement is entered into for the benefit of the State of California, which shall have the right to enforce this agreement. This agreement and any dispute arising under this agreement shall be governed by the laws of the State of California. This

agreement and the certifications contained herein shall survive the expiration or termination of Recipient Institution and/or Principal Investigator's right to custody of CCR data. Any dispute that arises under or relates to this agreement shall be resolved in the State of California, Superior Court for the county in which the CCR Data custodian is located or, at the option of the State of California, Sacramento County Superior Court. In any litigation or other proceeding by which one party seeks to enforce its rights under this agreement or seeks a declaration of any rights or obligations under this agreement, the prevailing party shall be awarded reasonable attorney fees, together with any costs and expenses, to resolve the dispute and to enforce the final judgment.

20. Notwithstanding any other provision of this agreement, the CCR Data Custodian shall have no obligation to provide CCR data to Recipient Institution unless and until this agreement is approved by the Chief, Chronic Disease Surveillance and Research Branch, California Department of Public Health.

For Recipient Institution:

I have read the foregoing agreement. I have the authority to execute this confidentiality agreement on behalf of the Recipient Institution. By signing below I make the agreements, and certifications contained therein on behalf of the Recipient Institution. I understand that these are material representations of fact upon which reliance was placed when this transaction was entered into.

_____ _____

Signature Dated

_____

Printed Name and Title

Principal Investigator:

I have read and understood the foregoing agreement.

_____ _____

Signature Dated

_____

Printed Name and Title

APPROVAL BY CALIFORNIA DEPARTMENT OF PUBLIC HEALTH, CHRONIC DISEASE SURVEILLANCE AND RESEARCH BRANCH:

_____ _____

Signature Dated

_____

Printed Name and Title

Appendix 4: Example Confidentiality Pledge

Employee Confidentiality Pledge

Confidentiality Protection Guidelines

Data collection, quality control, and research in which you will participate in one way or another are based upon the analysis of personal medical information on patients and research subjects. Therefore, the protection of such information is the responsibility of each member of the staff. As a staff member, you must understand that a breach of the confidentiality at any level is cause for immediate disciplinary action.

Responsibility for preserving confidentiality includes not merely passive acknowledgment of the procedures described below, but the active support of these procedures at all times. Accidental breaches will not be excused. Confidential information includes all patient, research subject, physician, and health care facility data. All such information is to be treated as medically privileged.

1. All employees are required to read and sign the *Employee Confidentiality Pledge* on their first day of employment and annually thereafter, and to abide by its guidelines. The *Employee Confidentiality Pledge* is then witnessed by the employee's supervisor. The Pledge is then placed in the employee's personnel file. Breach of this Pledge subjects the employee to immediate disciplinary action.

2. After signing the *Employee Confidentiality Pledge,* the employee is given a user name and password to log onto a network computer. If database access is required, a user name and password for database access will be assigned. All access passwords are considered confidential and are not to be shared.

3. Safeguards must be maintained to protect the medically sensitive and confidential information on all patients and research subjects whose information is contained in the California Cancer Registry databases. All cancer patient data are protected by the confidentiality requirements of the California Health and Safety Code, Sections 100330 and 103885. The confidentiality of medical information is further protected under provisions of the Government Code, Sections 6250-6265 (California Public Records Act). Provisions of the Civil Code, Section 1798–1798.70 (Information Practices Act), govern the release of personal identifiers or information that may allow identification of an individual. Therefore, personal identifiers as defined above should not be transmitted or published through e-mail, publications, presentations or any other public medium.

4. All files on patients and research participants are kept in locked file cabinets or in the locked confidential records room. Extra keys to staff file cabinets are to be available when needed but are to be kept inside the locked records room and never loose inside unlocked desk drawers. No confidential data should remain on top of desk after working hours. All lockable office doors should be closed and locked.

5. Office space will be secured and access to the premises limited to staff and authorized visitors. It is the responsibility of the staff member to make sure that no confidential data are visible to visitors.

6. All confidential data must be protected in a manner consistent with the current guidelines established by the institution and in accordance to requirements for access or use of CCR data.

7. A confidential fax cover sheet must be used when a staff member faxes confidential information. The recipient is to be notified in advance by telephone that confidential information is being transmitted, and the recipient should wait by the fax machine to retrieve the fax. The staff member should confirm that the fax has been received.

8. When mailing confidential information, staff members must place the confidential data inside an envelope, seal the envelope, stamp it "confidential," and place it in a mailing envelope. Also stamp "confidential" on the enclosed business reply envelope and on the mailing envelope.

9. When an employee is finished with computer printouts and other documents that contain confidential information, the documents are to be locked up or shredded.

10. Any breach of confidentiality must be reported immediately to your supervisor.

11. When employees are no longer employed by the institution, computer accounts (user ID and password) will be terminated and keys to buildings and offices will be returned to Administration. Terminated employees are admonished that their work has been confidential in nature, and this confidentiality should continue to be followed.

Confidentiality Protection Pledge

As a staff member of this institution, I give my personal assurance that I have read, understand, and will adhere to this *EMPLOYEE CONFIDENTIALITY PLEDGE.* I further understand that a breach of confidentiality, as described in the Pledge, is cause for disciplinary action.

_____	_____	_____
Staff Member (printed name)	Staff Member (signature)	Date

_____	_____
Supervisor	Date

Patient Data Confidentiality Guidelines

Help protect confidential data from unauthorized disclosure by:

In the Cubicle/Office

- Lock the computer by pressing the Windows + L key at the same time or by using CTL-ALT-DEL to bring up the Windows Security screen, and click on the “Lock Computer” button.
- Close confidential applications, such as Eureka, before you leave your cubicle/office for lunch or breaks.
- Face monitor away from the door to prevent viewing by unauthorized individuals.
- Keep all printed confidential data in confidential folders when not using it. Lock up all confidential folders with data when leaving the vicinity of your cubicle/office for more than a minute.
- Shred all printed confidential data when finished with it.
- Place all printed confidential data in folders and minimize all workstation screens containing confidential data when outside visitors are in your cubicle/office.

In the Break Room or Halls

- Do not discuss confidential data.
- Do not carry confidential data with you when using the break room or restroom.

In the Copy/Work Area

- Pick up all printouts promptly. If you walk by the printer, check any printouts of confidential data waiting to be picked up. If the owner can't be identified, place it in a confidential folder and give it to one of the administrative staff.
- Fax confidential data with a cover sheet marked "Confidential". Verify the fax number, send only to fax machines secured for confidential data, use the minimum amount of data possible, and make sure that somebody is waiting for the fax to arrive. For USPS or courier transport of confidential data, put the data in a sealed envelope marked "Confidential" with the recipient's name and then place the confidential envelope inside the mailing envelope. If digital media (CD, tape, USB drive) is being sent, encrypt the data with a strong password and send the password through other means.

Internet

- Use web browsing only for approved business uses
- Only open email from known trusted senders
- Verify email attachments with sender before opening
- Do not send confidential data over the Internet or email unless appropriately encrypted.

Computer

- Do not send or accept any data that is not appropriately encrypted.
- Use commercial grade encryption for email attachments, file transfer applications, laptop hard drives and other media like CD/DVDs, tape backup, USB keys, etc. that may contain confidential data. If possible encrypt confidential data on workstation and server drives.

- Remove all confidential data when no longer needed.
- Make sure that all OS and Office software security updates are applied.
- Use a commercial grade antivirus program and keep it up to date
- Follow IT guidelines for creating and changing workstation passwords.
- Memorize or carefully guard all passwords.
- Keep portable computers and storage media with you when travelling. Do not leave in cars, hotels or checked baggage.

Office Entry Doors

- Do not let anyone in the office you don't know, even if he/she appears to have an electronic key card.
- Do not prop open doors.
- Lock the front doors with the keys and set the alarm if you are the last one leaving the building.
- Instruct visitors to sign in and wear a visitor badge.
- Escort visitors back and forth to the door and instruct them to sign out and return the visitor badge.

Non-work Related Patient Look-up

- Do not do it.

Appendix 5: Patient Record Request Form

Mail Requests to:
Chronic Disease Surveillance and Research Branch
California Cancer Registry
1631 Alhambra Blvd., Suite 200
Sacramento, CA 95816

INDIVIDUAL WHOSE INFORMATION YOU ARE REQUESTING
*Patient Name:
Patient Alias Name:
*Patient Social Security Number:
*Patient Date of Birth:
*Patient Date of Diagnosis:
*Type of Cancer:
*Patient Date of Death (if applicable): **CERTIFIED DEATH CERTIFICATE MUST BE ATTACHED (with raised seal)**
Patient Address at Diagnosis:
*Patient County of Diagnosis:
**required fields*

REPRESENTATIVE CONTACT INFORMATION		
Last Name:	First Name:	Middle Initial:
Physical Address:	City/State:	Zip Code:
Mailing Address (if different):	City/State:	Zip Code:
Daytime Phone Number:	Email Address:	Please return all certified copies: ☐ Yes ☐ No

WHAT LEGAL AUTHORITY DO YOU HAVE TO REQUEST HEALTH INFORMATION:	
☐ Self	☐ Conservator
☐ Parent	☐ Executor of Will
☐ Guardian	☐ Other (Please specify – spouse, son, daughter, etc):

☐ Medical Power of Attorney	
NOTE: You must attach all LEGAL documentation to verify that you have legal authority to access the patient's records (Please refer to the CCR Patient Record Request Check List).	

IDENTIFYING INFORMATION REQUIRED
☐ Copy of Identification Attached Type: _____ (Driver's License, Identification Card, Birth Certificate) ☐ Address Verification Attached TYPE: _____ (Utility Bill, Phone Bill, Driver's License, Etc.)
IF NO IDENTIFICATION IS ATTACHED, YOUR SIGNATURE MUST BE NOTARIZED. Notarized by _____on _____ (Date) Notary Public Number _____ **UNOFFICIAL UNLESS STAMPED BY NOTARY PUBLIC**
I DECLARE UNDER PENALTY OF PERJURY THAT THE INFORMATION ON THIS FORM IS TRUE AND CORRECT. Representative Signature: Date:

Appendix 6: CCR Patient Record Request Check List

The following items must be submitted to request a record:

- **California Cancer Registry Patient Record Request Form (Version 2.2) with the following required information:**
    - Patient Name
    - Patient Social Security Number
    - Patient Date of Birth
    - Patient Date of Diagnosis
    - Type of Cancer
    - Patient Date of Death (if applicable)
    - Patient County of Diagnosis
    - Signature
    - Relation to patient
    - Contact Information (please provide a physical address where documents can be delivered, a signature will be required at time of delivery)

- **If requesting patient record for self:**
    - California Cancer Registry Patient Record Request Form
    - Copy of Identification (driver's license, official state-issued identification card, passport, certified copy of birth certificate, etc.)
    - Address Verification (copy of phone bill, utility bill, driver's license, etc.)

- **If requesting a deceased patient's record:**
    - California Cancer Registry Patient Record Request Form
    - Certified death certificate (with the raised seal)
    - Legal document establishing your legal authority
        a) If you are the surviving spouse and named on the death certificate, ONLY a certified copy of the death certificate is required to establish legal authority
        b) For any requestor other than the surviving spouse, a certified copy of one of the following is required to establish legal authority:
            - ✓ Letters Testamentary
            - ✓ Letters of Administration
            - ✓ Letters of Administration with Will Annexed
            - ✓ Order Authorizing Independent Administration of Estate
            - ✓ Spouse or Domestic Partner Property Order
            - ✓ Order Setting Aside Decedent's Estate to the Decedent's Surviving Spouse and Minor Children
            - ✓ Judgment of Final Distribution
            - ✓ Trust Document
    - Copy of Identification (driver's license, official state-issued identification card, passport, certified copy of birth certificate, etc.)
    - Address Verification (copy of phone bill, utility bill, driver's license, etc.)

- **If requesting a patient's record on behalf of living patient:**
    - California Cancer Registry Patient Record Request Form
    - Legal document establishing your legal authority (Power of Attorney)
    - Copy of Identification (driver's license, official state-issued identification card, passport, certified copy of birth certificate, etc.)
    - Address Verification (copy of phone bill, utility bill, driver's license, etc.)

□ Mail Requests to:

Chronic Disease Surveillance and Research Branch
California Cancer Registry
1631 Alhambra Blvd., Suite 200
Sacramento, CA 95816

□ Questions or concerns, please contact:

California Cancer Registry
Phone: (916) 731-2500
Fax: (916) 454-1538