California Department of Public Health – California Cancer Registry

Data Use and Disclosure Agreement (Research)

This Data Use Agreement (Agreement) is between the California Department of Public Health, Chronic Disease Surveillance and Research Branch, Cancer Registry ("CDPH") and _____ [NAME OF DATA RECIPIENT] ("Recipient") and sets forth the information privacy and security requirements Recipient is obligated to follow with respect to all data from California Cancer Registry ("CCR Data") disclosed to Recipient. CDPH and Recipient desire to protect the privacy and provide for the security of CCR Data pursuant to this Agreement, in compliance with state and federal laws applicable to CCR Data.

I. Order of Precedence: With respect to information privacy and security requirements for all CCR Data, the terms and conditions of this Agreement shall take precedence over any conflicting terms or conditions set forth in any other agreement between Recipient and CDPH.

II. Effect on Lower Tier Transactions: The terms of this Agreement shall apply to all contracts, subcontracts, and subawards, and the information privacy and security requirements Recipient is obligated to follow with respect to CCR Data disclosed to Recipient pursuant to Recipient's agreement with CDPH. When applicable Recipient shall incorporate the relevant provisions of this Agreement into each subcontract or subaward to its agents, subcontractors, or independent consultants.

III. Definitions: For purposes of the Agreement between Recipient and CDPH, the following definitions shall apply:

A. Breach:

"Breach" means:

1. the unauthorized acquisition, access, use, or disclosure of CCR Data in a manner which compromises the security, confidentiality, or integrity of the information; or

2. the same as the definition of "breach of the security of the system" set forth in California Civil Code section 1798.29(f).

B. Confidential Information: "Confidential information" means information that:

1. does not meet the definition of "public records" set forth in California Government Code section 7920.530, or is exempt from disclosure under any of the provisions of Section 7921.000, et seq. of the California Government Code or any other applicable state or federal laws; or

2. is contained in documents, files, folders, books, or records that are clearly labeled, marked, or designated with the word "confidential" by CDPH.

C. CCR Data: CCR Data means Confidential Information collected and maintained by CCR pursuant to Health and Safety Code section 103885(g), excluding data or information pertaining to veterans of the United States Armed Forces.

D. Disclosure: "Disclosure" means the release, transfer, provision of, access to, or divulging in any manner of information outside the entity holding the information.

E. Personal Information: "Personal information" means information, in any medium (paper, electronic, oral) that:

1. directly or indirectly collectively identifies or uniquely describes an individual or

2. could be used in combination with other information to indirectly identify or uniquely describe an individual or link an individual to the other information; or

3. meets the definition of "personal information" set forth in California Civil Code section 1798.3, subdivision (a) or

4. is one of the data elements set forth in California Civil Code section 1798.29, subdivision (g)(1) or (g)(2); or

5. meets the definition of "medical information" set forth in either California Civil Code section 1798.29, subdivision (h)(2) or California Civil Code section 56.05, subdivision (j); or

6. meets the definition of "health insurance information" set forth in California Civil Code section 1798.29, subdivision (h)(3); or

7. is protected from disclosure under applicable state or federal law.

F. Security Incident: "Security Incident" means:

1. an attempted breach; or

2. the attempted or successful unauthorized access or disclosure, modification, or destruction of CCR Data, in violation of any state or federal law or in a manner not permitted under this Agreement; or

3. the attempted or successful modification or destruction of, or interference with, Recipient's system operations in an information technology system that negatively impacts the confidentiality, availability, or integrity of CCR Data; or

4. any event that is reasonably believed to have compromised the confidentiality, integrity, or availability of an information asset, system, process, data storage, or transmission. Furthermore, an information security incident may also include an event that constitutes a violation or imminent threat of violation of information security policies or procedures, including acceptable use policies.

G. Use: "Use" means the sharing, employment, application, utilization, examination, or analysis of CCR Data.

H. Workforce Member: "Workforce Member" means an employee, volunteer, trainee, or other person whose conduct, in the performance of work for Recipient, is under the direct control of Recipient, whether or not they are paid by Recipient.

IV. No HIPAA Business Associate Agreement or Relationship Between the Parties: This Agreement and the relationship it memorializes between the Parties does not constitute a business associate agreement or business associate relationship pursuant to Title 45, C.F.R., Part 160.103 (definition of "business associate"). The basis for this determination is Section 160.203(c) of Title 45 of the Code of Federal Regulations (see, also, [HITECH Act, § 13421, subdivision. (a)].). Accordingly, this Agreement is not intended to nor at any time shall it result in or be interpreted or construed as to create a business associate relationship between the Parties.

V. Background and Purpose: Recipient desires to obtain CCR Data for the purposes set forth in the Recipient's Application for Disclosure of California Cancer Registry Data and the letters of approval issued by the Recipient's institutional review board ("IRB Approval"), and the Committee for the Protection of Human Subjects (CPHS) for the California Health and Human Services Agency (CalHHS) or an independent review board approved by CPHS, attached hereto as Attachment 1. Information and data disclosed to the Recipient shall be used only for statistical, scientific, medical research, and public health purposes that are described in Attachment 1, and the Recipient's data sharing plan also described in Attachment 1. Usage of the Data by the Recipient outside the approvals in Attachment 1 requires review by CDPH for amendment of this Agreement as appropriate.

VI. Disclosure Restrictions: Recipient and its employees, agents, and subcontractors shall protect from unauthorized disclosure of any CCR Data. Recipient shall not disclose, except as otherwise specifically permitted by this Agreement between Recipient and CDPH, CCR Data to anyone other than CDPH personnel or programs without prior written authorization from the CDPH Program Contract Manager, except if disclosure is required by State or Federal law. In the event Recipient receives a subpoena or other compulsory legal process compelling disclosure of CCR Data, Recipient shall notify CCR within twenty-four (24) hours of receipt of the subpoena or other compulsory legal process, and Recipient shall take legal steps to oppose the subpoena or other compulsory legal process at its sole expense.

a. Permitted Secondary Data Disclosure:

Recipient may only redisclose CCR Data received under this Agreement if the Recipient is required to participate in data sharing with federal or federally designated data repositories and with other researchers, as described in Attachment 1. Any CCR Data that will be redisclosed by Recipient as permitted in this section shall be de-identified pursuant to the California Health and Human Services Agency Data De-Identification

Guidelines (CalHHS DDG), which can be accessed here: CalHHS Data De-Identification Guidelines.

VII. Legal Authority: The legal authority for CDPH to collect, create, access, use, and disclose CCR Data to the Recipient and the Recipient's use of CCR Data is Health and Safety Code section 103885 and Civil Code section 1798.24.

VIII. Use Restrictions: Recipient and its employees, agents, and subcontractors shall not use any CCR Data for any purpose other than as permitted under this Agreement.

IX. Safeguards: Recipient shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the privacy, confidentiality, security, integrity, and availability of CCR Data, including electronic or computerized data. At each location where CCR Data exists under Recipient's control, Recipient shall develop and maintain a written information privacy and security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of Recipient's operations and the nature and scope of its activities in performing this Agreement, and which incorporates the requirements of Section X, Security, below. Recipient shall provide CDPH with the Recipient's current and updated policies within five (5) business days of a request by CDPH for the policies.

X. Security: Recipient shall take any and all steps reasonably necessary to ensure the continuous security of all computerized data systems containing CCR Data. These steps shall include, at a minimum, complying with all of the data system security precautions listed in Recipient Data Security Standards set forth in Attachment 2 to this Agreement.

XI. Security Officer: At each place where CCR Data is located, Recipient shall designate in Attachment 3 hereto a Security Officer to oversee its compliance with this Agreement and to communicate with CDPH on matters concerning this Agreement.

XII. Training: Recipient shall provide training on its obligations under this Agreement, at its own expense, to all of its employees who assist in the performance of Recipient's obligations under Recipient's agreement with CDPH, including this Agreement or otherwise use or disclose CCR Data.

A. Recipient shall require each employee who receives training to certify, either in hard copy or electronic form, the date on which the training was completed.

B. Recipient shall retain each employee's certifications for CDPH inspection for a period of three years following this Agreement's termination or completion.

C. Recipient shall provide CDPH with its employee's certifications within five (5) business days of a request by CDPH for the employee's certifications.

XIII. Workforce Member Discipline: Recipient shall impose discipline that it deems appropriate (in its sole discretion) on such employees and other Recipient workforce members under

Recipient's direct control who intentionally or negligently violate any provisions of this Agreement.

XIV. Breach and Security Incident Responsibilities:

A. Notification to CDPH of Breach or Security Incident: Recipient shall notify CDPH **immediately by telephone call plus email** upon the discovery of a breach (as defined in this Agreement) and **within twenty-four (24) hours by email** of the discovery of any security incident (as defined in this Agreement) unless a law enforcement agency determines that the notification will impede a criminal investigation, in which case the notification required by this section shall be made to CDPH immediately after the law enforcement agency determines that such notification will not compromise the investigation. The notification shall be provided to the CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer using the contact information listed in Section XIV (F) below. If the breach or security incident is discovered after business hours or on a weekend or holiday and involves data in electronic or computerized form, notification to CDPH shall be provided by calling the CDPH Information Security Office at the telephone numbers listed in Section XIV (F) below. For purposes of this Section, breaches and security incidents shall be treated as discovered by Recipient as of the first day on which such breach or security incident is known to Recipient or, by exercising reasonable diligence, would have been known to Recipient. Recipient shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee or agent of Recipient.

Recipient shall take:

1. prompt corrective action to mitigate any risks or damages involved with the breach or security incident and to protect the operating environment; and

2. any action pertaining to a breach is required by applicable federal and state laws, including, specifically, California Civil Code section 1798.29.

B. Investigation of Breach and Security Incidents: Recipient shall immediately investigate such breach or security incident. As soon as the information is known and subject to the legitimate needs of law enforcement, the Recipient shall inform the CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer of:

1. what data elements were involved, and the extent of the data disclosure or access involved in the breach, including, specifically, the number of individuals whose Personal Information was breached; and

2. a description of the unauthorized persons known or reasonably believed to have improperly used the CCR Data and/or a description of the unauthorized persons known or reasonably believed to have improperly accessed or acquired the CCR Data or to whom it is known or reasonably believed to have had the CCR Data improperly disclosed to them; and

3. a description of where the CCR Data is believed to have been improperly used or disclosed and

4. a description of the probable and proximate causes of the breach or security incident; and

5. whether Civil Code section 1798.29 or any other federal or state laws requiring individual notifications of breaches have been triggered.

C. Written Report: Recipient shall provide a written report of the investigation to the CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer as soon as practicable after the discovery of the breach or security incident. The report shall include, but not be limited to, the information specified above, as well as a complete, detailed corrective action plan, including information on measures that were taken to halt and/or contain the breach or security incident and measures to be taken to prevent the recurrence or further disclosure of data regarding such breach or security incident.

D. Notification to Individuals: If notification to individuals whose information was breached is required under state or federal law, and regardless of whether the Recipient is considered only a custodian and/or non-owner of the CCR Data, the Recipient shall, at its sole expense, and at the sole election of CDPH, either:

1. make notification to the individuals affected by the breach (including substitute notification), pursuant to the content and timeliness provisions of such applicable state or federal breach notice laws. Recipient shall inform the CDPH Privacy Officer of the time, manner, and content of any such notifications prior to the transmission of such notifications to the individuals or

2. cooperate with and assist CDPH in its notification (including substitute notification) to the individuals affected by the breach.

E. Submission of Sample Notification to Attorney General: If notification to more than 500 individuals is required pursuant to California Civil Code section 1798.29, and regardless of whether the Recipient is considered only a custodian and/or non-owner of the CCR Data, the Recipient shall, at its sole expense, and at the sole election of CDPH, either:

1. electronically submit a single sample copy of the security breach notification, excluding any personally identifiable information, to the Attorney General pursuant to the format, content, and timeliness provisions of Section 1798.29, subdivision (e). Recipient shall inform the CDPH Privacy Officer of the time, manner, and content of any such submissions prior to the transmission of such submissions to the Attorney General or

2. cooperate with and assist CDPH in its submission of a sample copy of the notification to the Attorney General.

F. CDPH Contact Information: To direct communications to the above-referenced CDPH staff, the Recipient shall initiate contact as indicated herein. CDPH reserves the right to make changes

to the contact information below by verbal or written notice to the Recipient. Said changes shall not require an amendment to this Agreement.

CDPH Program Contract Manager	CDPH Privacy Officer	CDPH Chief Information Security Officer
Mark Damesyn, MPH, DrPH Chief, Chronic Disease Surveillance and Research Branch/Center for Healthy Communities/California Department of Public Health Telephone: 530-304-1272 Email: mark.damesyn@cdph.ca.gov	Privacy Officer Privacy Office Office of Legal Services California Dept. of Public Health P.O. Box 997377, MS 0506 Sacramento, CA 95899-7377 Email: privacy@cdph.ca.gov Telephone: (877) 421-9634	Chief Information Security Officer Information Security Office California Dept. of Public Health P.O. Box 997377, MS6302 Sacramento, CA 95899-7413 Email: cdphiso@cdph.ca.gov Telephone: (855) 500-0016

XV. Documentation of Disclosures for Requests for Accounting: Recipient shall document and make available to CDPH or (at the direction of CDPH) to an Individual, such disclosures of CCR data and information related to such disclosures necessary to respond to a proper request by the subject Individual for an accounting of disclosures of Personal Information as required by Civil Code section 1798.25 and Confidential Information pursuant to Health and Safety Code section 103885, or any applicable state or federal law.

XVI. Requests for CCR Data by Third Parties: Recipient and its employees, agents, or subcontractors shall promptly transmit to the CDPH Program Contract Manager all requests for disclosure of any CCR Data requested by third parties to this Agreement between Recipient and CDPH (except from an Individual for an accounting of disclosures of the individual's Personal Information pursuant to applicable state or federal law) unless prohibited from doing so by applicable state or federal law.

XVII. Audits, Inspection, and Enforcement: CDPH may inspect the facilities, systems, books, and records of the Recipient to monitor compliance with this Agreement. Recipient shall promptly remedy any violation of any provision of this Agreement and shall certify the same to the CDPH Program Contract Manager in writing.

XVIII. Term: The term of this Agreement shall commence on the date below and remain in effect until the expiration of the IRB Approval, Attachment 1. Any use of CCR Data pursuant to an amendment or extension of the IRB approval shall be memorialized in an amendment to this Agreement. Upon the expiration of the IRB Approval, all research activities involving the use of CCR Data must cease immediately unless an amendment or extension of the IRB approval has been obtained and documented.

XIX. Termination for Cause:

A. Termination upon Breach: A breach by Recipient of any provision of this Agreement, as determined by CDPH, shall constitute a material breach of the Agreement and grounds for

immediate termination of this Agreement by CDPH. At its sole discretion, CDPH may give the Recipient 30 days to cure the breach.

B. Judicial or Administrative Proceedings: Recipient will notify CDPH if it is named as a defendant in a criminal proceeding related to a violation of this Agreement. CDPH may terminate the Agreement if the Recipient is found guilty of a criminal violation related to a violation of this Agreement. CDPH may terminate this Agreement if a finding or stipulation that the Recipient has violated any security or privacy laws is made in any administrative or civil proceeding in which the Recipient is a party or has been joined.

XX. Return or Destruction of CCR Data on Expiration or Termination: Upon expiration or termination of this Agreement, Recipient shall securely return or destroy the CCR Data. If return or destruction is not feasible, the Recipient shall provide a written explanation to the CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer using the contact information listed in Section XIV (F) above.

A. Retention: If required by state or federal law, the Recipient may retain, after termination of this Agreement, CCR Data for the time specified as necessary to comply with the law.

B. Obligations Continue Until Return or Destruction: Recipient's obligations under this Agreement shall continue until Recipient destroys the CCR Data or returns the CCR Data to CDPH; provided, however, that on expiration or termination of this Agreement between Recipient and CDPH, Recipient shall not further use or disclose the CCR Data except as required by state or federal law or specified in the Agreement.

C. Notification of Election to Destroy CCR: If the Recipient elects to destroy the CCR Data, the Recipient shall certify in writing to the CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer, using the contact information listed in Section XIV (F), above, that the CCR Data has been securely destroyed. The notice shall include the date and type of destruction method used.

XXI. Amendment: The parties acknowledge that federal and state laws regarding information security and privacy rapidly evolve, and that amendment of this Agreement may be required to provide for procedures to ensure compliance with such laws. The parties specifically agree to take such action as is necessary to implement new standards and requirements imposed by regulations and other applicable laws relating to the security or privacy of CCR Data. The parties agree to promptly enter into negotiations concerning an amendment to this Agreement consistent with new standards and requirements imposed by applicable laws and regulations.

XXII. Assistance in Litigation or Administrative Proceedings: Recipient shall make itself and any subcontractors, workforce employees, or agents assisting Recipient in the performance of its obligations under this Agreement between Recipient and CDPH available to CDPH at no cost to CDPH to testify as witnesses, in the event of litigation or administrative proceedings being commenced against CDPH, its director, officers, or employees based upon claimed violation of laws relating to security and privacy, which involves inactions or actions by Recipient, except where Recipient or its subcontractor, workforce employee, or agent is a named adverse party.

XXIII. Costs and Means of Transmitting CCR Data: Recipient shall pay CCR's costs for providing CCR Data to Recipient in accordance with the current data preparation costs schedule available on CCR's website. Upon receipt of payment for costs, CCR will provide the Recipient with the requested CCR Data. CCR 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 Recipient using CDPH approved secure email system. If the CCR Data file is too large to send via email, the file will be saved on a CD and shipped overnight to the Recipient via a company that is bonded and provides tracking information on the shipment, i.e., UPS, FEDEX or Golden State Overnight, at Recipient's expense using Recipient's account.

XXIV. No Third-Party Beneficiaries: Nothing express or implied in the terms and conditions of this Agreement is intended to confer, nor shall anything herein confer, upon any person other than CDPH or Recipient and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

XXV. Interpretation: The terms and conditions in this Agreement shall be interpreted as broadly as necessary to implement and comply with regulations and applicable State laws. The parties agree that any ambiguity in the terms and conditions of this Agreement shall be resolved in favor of a meaning that complies and is consistent with federal and state laws and regulations.

XXVI. Survival: If Recipient does not return or destroy the CCR Data upon the completion or termination of this Agreement, the respective rights and obligations of Recipient under Sections IX, X, and XIV of this Agreement shall survive the completion or termination of this Agreement between Recipient and CDPH.

XXVII. Choice of Law and Venue: The laws of the state of California will govern any dispute from or relating to this Agreement. The parties submit to the exclusive jurisdiction of the state of California and federal courts for or in Sacramento and agree that any legal action or proceeding relating to the Agreement may only be brought in those courts.

XXVIII. Entire Agreement: This Agreement, including all attachments, constitutes the entire agreement between CCR and Recipient. Any and all modifications of this Agreement must be in writing and signed by all parties. Any oral representations or agreements between the parties shall be of no force or effect.

XXIX. Signatures:

IN WITNESS, WHEREOF, the Parties have executed this Agreement as follows:

The undersigned individual hereby attests that they are authorized to enter into this Agreement on behalf of the Data Recipient Institution and agrees to abide by and enforce all the terms specified herein.

For Recipient Institution:

_____

(Name of Recipient Institutional Representative)

_____

(Title)

_____

(Signature) (Date)

Recipient:

I have read and understood the foregoing agreement.

_____

(Name of Recipient)

_____

(Title)

_____

(Signature) (Date)

On behalf of CDPH, the undersigned individual hereby attests that they are authorized to enter into this Agreement and agrees to all the terms specified herein.

Mark Damesyn, M.P.H., Dr.P.H.
Chief, Chronic Disease Surveillance and Research Branch
Center for Healthy Communities
California Department of Public Health

_____

(Signature) (Date)

Attachment 1

Recipient's Application for the Disclosure of Confidential California Cancer Registry Data and the letters of approval issued by the Recipient's IRB and the Committee for the Protection of Human Subjects (CPHS) for the California Health and Human Services Agency (CalHHS) or a CPHS approved independent review board.

Attachment 2

Recipient Data Security Standards

I. Personnel Controls

A. *Workforce Members Training and Confidentiality*. Before being allowed access to CCR Data, the Recipient's workforce members who will be granted access to CCR data must be trained in their security and privacy roles and responsibilities at the Recipient's expense and must sign the confidentiality agreement attached hereto as Attachment 4. Training must be on an annual basis. Acknowledgments of completed training and confidentiality statements, which have been signed and dated by workforce members, must be retained by the Recipient for a period of three (3) years following this Agreement's termination. Recipient shall provide the acknowledgements within five (5) business days to CDPH if so requested.

B. *Workforce Members Discipline*. Appropriate sanctions, including termination of employment where appropriate, must be applied against workforce members who fail to comply with privacy policies and procedures, acceptable use agreements, or any other provisions of these requirements.

C. *Workforce Member Assessment*. As permitted or required by law, the Recipient shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of this Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud or otherwise convicted of any felony or any misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Recipient shall promote and maintain an awareness of the importance of securing the CCR Data among the Recipient's employees and agents. Recipient shall retain the workforce member's assessment documentation for a period of three (3) years following termination of this Agreement.

II. Technical Security Controls

A. *Encryption*.

- All desktop computers and mobile computing devices must be encrypted in accordance with CDPH Cryptographic Standards or using the latest FIPS 140 validated cryptographic modules.

- All electronic files that contain CCR Data must be encrypted when stored on any removable media type device (such as USB thumb drives, CD/DVD, tape backup, etc.), in accordance with CDPH Cryptographic Standards or using the latest FIPS 140 validated cryptographic modules.

- CCR Data must be encrypted during data in transit and at rest on all public telecommunications and network systems and at all points not in the direct ownership and control of CDPH, in accordance with CDPH Cryptographic Standards or using the latest FIPS 140 validated cryptographic modules.

B. *Server Security*. Servers containing unencrypted CCR Data must have sufficient local and network perimeter administrative, physical, and technical controls in place to protect the CCR Data based on a current risk assessment/system security review.

C. *Minimum Necessary*. Only the minimum amount of CCR Data required to complete an authorized task or workflow may be copied, downloaded, or exported to any individual device.

D. *Antivirus software*. Recipient shall employ automatically updated malicious code protection mechanisms (anti-malware programs or other physical or software-based solutions) at its network perimeter and at workstations, servers, or mobile computing devices to continuously monitor and take action against system or device attacks, anomalies, and suspicious or inappropriate activities.

E. *Patch Management*. All devices that process or store CCR Data must have a documented patch management process. Vulnerability patching for Common Vulnerability Scoring System (CVSS) "Critical" severity ratings (CVSS 9.0 – 10.0) shall be completed within forty-eight (48) hours of publication or availability of vendor-supplied patch; "High" severity rated (CVSS 7.0- 8.9) shall be completed within seven (7) calendar days of publication or availability of vendor-supplied patch; all other vulnerability ratings (CVSS 0.1 – 6.9) shall be completed within thirty (30) days of publication or availability of vendor-supplied patch, unless prior ISO and PO variance approval is granted.

F. *User Identification and Access Control.* All Recipient workforce members must have a unique local and/or network user identification (ID) to access CCR Data. To access systems/applications that store, process, or transmit CCR Data, they must comply with SIMM 5360-C Multi-factor Authentication (MFA) Standard and NIST SP800-63B Digital Identity Guidelines. The SIMM 5350-C provides steps for determining the Authenticator Assurance Level (AAL) and a set of permitted authenticator types for each AAL (0-3). Note: The MFA requirement does not apply to AAL 0.

All Recipient workforce members are required to leverage FIDO authentication. The FIDO authentication is AAL 3 compliance. FIDO certified devices such as YubiKeys and Windows Hello for Business (WHfB) are the mechanism for user authentication at CDPH.

Should a workforce member no longer be authorized to access CCR Data, or an ID has been compromised, that ID shall be promptly disabled or deleted. User IDs must integrate with user role-based access controls to ensure that individual access to CCR Data is commensurate with job-related responsibilities.

	AAL 1	**AAL 2**	**AAL 3**
Permitted Authenticator Types	- Memorized Secret - Look-Up Secret - Out-of-Band Devices	- Multi-Factor OTP Device - Multi-Factor Cryptographic Software	- Multi-Factor Cryptographic Device - Single-factor cryptographic Device used in conjunction

	- Single-Factor One-Time Password (OTP) Device - Multi-Factor OTP Device - Single-Factor Cryptographic Software - Single-Factor Cryptographic Device - Multi-Factor Cryptographic Software - Multi-Factor Cryptographic Device	- Multi-Factor Cryptographic Device - Memorized Secret **plus**: - Look-Up Secret - Out-of-Band Device - Single-Factor OTP Device - Single-Factor Cryptographic Software - Single-Factor Cryptographic Device	with Memorized Secret - Multi-factor OTP device (software or hardware) used in conjunction with a Single-Factor Cryptographic Device - Multi-factor OTP device (hardware only) used in conjunction with a Single-Factor Cryptographic Software - Single-factor OTP device (hardware only) used in conjunction with a Multi-Factor Cryptographic Software Authenticator - Single-Factor OTP device (hardware only) used in conjunction with a Single-Factor Cryptographic Software Authenticator and a Memorized Secret.

G. ***CCR Data Destruction***. When no longer required for business needs or legal retention periods, all electronic and physical media holding CCR Data must be purged from the Recipient's systems and facilities using the appropriate guidelines for each media type as described in the prevailing "National Institute of Standards and Technology – Special Publication 800-88" – "Media Sanitization Decision Matrix."

H. ***Reauthentication*****.** Recipient's computing devices holding or processing CCR Data must comply with the Reauthentication requirement, in which a session must be terminated (e.g., logged out) when the specified time is reached. Note: The reauthentication requirement does not apply to Authenticator Assurance Level (AAL) 0.

	AAL 1	**AAL 2**	**AAL 3**

Reauthentication	30 Days – Fix Period of Time, regardless of user activity	12 hours – Fix Period of Time, regardless of user activity; 30 minutes inactivity May use one of the authenticators to reauthenticate	12 hours – Fix Period of Time regardless of user activity; 15 minutes of inactivity Must use both authenticators to reauthenticate

In addition, reauthentication of individuals is required in the following situations:

- When authenticators change
- When roles change
- When the execution of a privileged function occurs (e.g., performing a critical transaction)

I. *Warning Banners*. During a user log-on process, all systems providing access to CCR Data must display a warning banner stating that the CCR Data is confidential, system and user activities are logged, and system and CCR Data use is for authorized business purposes only. Users must be directed to log off the system if they do not agree with these conditions.

J. *System Logging*. Recipient shall ensure its information systems and devices that hold or process CCR Data are capable of being audited and the events necessary to reconstruct transactions and support after-the-fact investigations are maintained. This includes the auditing necessary to cover related events, such as the various steps in distributed, transaction-based processes and actions in service-oriented architectures. Audit trail information relevant to the receipt, creation, modification, access to, and transmission of CCR Data must be stored with read-only permissions and be archived for six (6) years after the event occurrence. Recipients must protect audit information and audit logging tools from unauthorized access, modification, and deletion. There must also be a documented and routine procedure in place to review system logs for unauthorized access.

K. Live Data Usage. Using live data (production data) for testing and training purposes is not allowed. Synthetic data must be used. If synthetic data cannot be generated and/or used, a de-identification process against the live data must be done to reduce privacy risks to individuals. The de-identification process removes identifying information from a dataset so that individual data cannot be linked with specific individuals. Refer to CalHHS Data De-Identification Guidelines.

L. Privileged Access Management (PAM). Recipient is responsible for setting up and maintaining privileged accounts related to CCR Data and shall comply with the CDPH PAM Security Standard. Information resources include user workstations as well as servers, databases, applications, and systems managed on-premises and on the cloud.

M. *Intrusion Detection*. All Recipient systems and devices holding, processing, or transporting CCR Data that interact with untrusted devices or systems via the Recipient intranet and/or the internet must be protected by a monitored comprehensive intrusion detection system and/or intrusion prevention system.

III. Audit Controls

A. *System Security Review*. Recipient, to assure that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection for CCR Data, shall conduct at least an annual administrative assessment of risk, including the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of an information system or device holding, processing, or transporting CCR Data, along with periodic technical security reviews using vulnerability scanning tools and other appropriate technical assessments.

B. *Change Control*. All Recipient systems and devices holding, processing, or transporting CCR Data shall have a documented change control process for hardware, firmware, and software to protect the systems and assets against improper modification before, during, and after system implementation.

IV. Business Continuity / Disaster Recovery Controls

A. *Emergency Mode Operation Plan*. Recipient shall develop and maintain technical recovery and business continuity plans for systems holding, processing, or transporting CCR Data to ensure the continuation of critical business processes and the confidentiality, integrity, and availability of CCR Data following an interruption or disaster event lasting more than twenty-four (24) hours.

B. *Data Backup Plan*. Recipient shall have a documented, tested, accurate, and regularly scheduled full backup process for systems and devices holding CCR Data.

V. Paper Document Controls

A. *Supervision of CCR Data*. CCR Data in any physical format shall not be left unattended at any time. When not under the direct observation of an authorized Recipient workforce member, the CCR Data must be stored in a locked file cabinet, desk, or room. It also shall not be left unattended at any time in private vehicles or common carrier transportation, and it shall not be placed in checked baggage on common carrier transportation.

B. *Escorting Visitors*. Visitors who are not authorized to see CCR Data must be escorted by authorized workforce members when in areas where CCR Data is present, and CCR Data shall be kept out of sight of visitors.

C. *Removal of CCR Data*. CCR Data in any format must not be removed from the secure computing environment or secure physical storage of the Recipient, except with express written permission of CCR.

Attachment 3

Recipient Breach and Security Incident Contact Information

The following Recipient contact information must be included in the executed Agreement

Recipient Program Manager	Recipient Privacy Officer	Recipient Chief Information Security Officer (and IT Service Desk)
[Name]	[Name]	[Name]
[Title]	[Title]	[Title]
[Address]	[Address]	[Address]
[Address 2]	[Address 2]	[Address 2]
[City]	[City]	[City]
[State, Zip Code]	[State, Zip Code]	[State, Zip Code]
[Telephone]	[Telephone]	[Telephone]
[Fax]	[Fax]	[Fax]
[E-mail]	[E-mail]	[E-mail]

Attachment 4

Confidentiality Agreement

By signing this Confidentiality Agreement, I agree to the following:

1. I have read the *Data Use Agreement* between the California Cancer Registry ("CCR") and the person or entity identified as the Recipient in said agreement ("DUA") and agree to be bound by the terms in it.

2. I will safeguard the confidentiality of all information contained in data provided by CCR ("CCR Data") to which I will be given access in accordance with the terms of the DUA, and I will not in any way divulge, copy, release, sell, loan, review, or alter any CCR Data except as within the scope of my duties.

3. I will only access CCR Data for which I have a need to know, and I will use that information only as needed to perform my duties.

4. I will promptly report activities by any individual or entity that I suspect may compromise the availability, integrity, security, or privacy of CCR Data to the Recipient and/or CCR.

5. I understand that ownership of CCR Data is vested solely in CCR.

6. I understand that violating applicable laws and regulations governing the use and disclosure of CCR Data may result in civil and criminal penalties.

Signature: _____ Date: _____

Print Name: _____

Please retain a copy for your records.