CalREDIE Data Use And Disclosure Agreement

This California Reportable Disease Information Exchange (**CalREDIE**) Data Use And Disclosure Agreement (hereinafter referred to as "Agreement") sets forth the information privacy and security requirements that **Humboldt County Health Department** (hereinafter "Data Recipient") is obligated to follow with respect to all CalREDIE System Data, and other personal and confidential information, (as each of these types of data and information are defined herein), disclosed to Data Recipient by the California Department of Public Health (hereinafter "CDPH"). (Such CalREDIE System Data and other personal and confidential information are also referred to herein collectively as "Protected Data".) This Agreement covers Protected Data in any medium (paper, electronic, oral) the Protected Data exist in. By entering into this Agreement, CDPH and Data Recipient desire to protect the privacy and provide for the security of all Protected Data in compliance with all state and federal laws applicable to the Protected Data. Permission to receive, use and disclose Protected Data requires execution of this Agreement that describes the terms, conditions and limitations of Data Recipient's collection, use and disclosure of the Protected Data.

I. Supersession: This Agreement supersedes Agreement Number __None__, dated __None__, between CDPH and Data Recipient.

II. Definitions: For purposes of this Agreement, the following definitions shall apply:

A. Breach: "Breach" means:

i. the acquisition, access, use, or disclosure of Protected Data, in any medium (paper, electronic, oral), in violation of any state or federal law or in a manner not permitted under this Agreement, that compromises the privacy, security or integrity of the information. For purposes of this definition, "compromises the privacy, security or integrity of the information" means poses a significant risk of financial, reputational, or other harm to an individual or individuals; or

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

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

1. does not meet the definition of "public records" set forth in California Government Code section 6252, subdivision (e), or is exempt from disclosure under any of the provisions of Section 6250, et seq. of he California Government Code or any other applicable state or federal laws; or
2. is "personal information" as defined in this Agreement.
3. Meets the definition of "Confidential public health record" set forth in California Health and Safety Code section 121035, subdivision (c); or

B. Disclosure: "Disclosure" means the release, transfer, provision of, access to, or divulging in any other manner of information.

C. California Reportable Disease Information Exchange (CalREDIE) System Data: "California Reportable Disease Information Exchange (CalREDIE) System Data" means data in or from the state-wide reportable disease database supported and maintained by CDPH of demographic, epidemiologic (including clinical information, risk factor and potential risk factor information, laboratory test and result information), and administrative information on reportable communicable diseases, known as the California Reportable Disease Information Exchange (CalREDIE). CalREDIE data specifically includes information contained in or extracted from the following:

1. Confidential Morbidity Report (CMR) required by Title 17 of the California Code of Regulations (CCR) Sections 2500, 2593, 2641.5-2643.20, and 2800-2812 Reportable Diseases and Conditions

2. Laboratory Test and Result information for required by Title 17 of the CCR Sections 2505 and 2641.5 - 2643.20
3. Communicable Disease Control Report Forms (required of the Local Health Jurisdictions by CDPH Administrative data collected in CalREDIE

D. Personal Information: "Personal information" means information that:

1. by itself directly identifies or uniquely describes an individual; or
2. creates a substantial risk that it 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, subdivisions (e)(1), (2) or (3); or
5. meets the definition of "medical information" set forth in either California Civil Code section 1798.29, subdivision (f)(2) or California Civil Code section 56.05, subdivision (g); or
6. meets the definition of "health insurance information" set forth in California Civil Code section 1798.29, subdivision (f)(3).

E. Security Incident: "Security Incident" means:

1. an attempted breach; or
2. the attempted or successful modification or destruction of Protected 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, Data Recipient's system operations in an information technology system, that negatively impacts the confidentiality, availability or integrity of Protected Data, or hinders or makes impossible Data Recipient's receipt, collection ,creation, storage, transmission or use of Protected Data by Data Recipient pursuant to this Agreement.

F. Use: "Use" means the sharing, employment, application, utilization, examination, or analysis of information.

III. Background and Purpose: The California Reportable Disease Information Exchange (CalREDIE) is a computer application that the CDPH is implementing for web-based disease reporting and surveillance. The purpose of this application is to improve the efficiency of surveillance activities and the early detection of public health events through the collection of more complete and timely surveillance information on a state wide basis. CalREDIE is a secure, web-based electronic solution for health care providers to report cases of conditions of public health interest; and for laboratories to report laboratory reports for notifiable conditions to LHDs and the CDPH. CalREDIE is an integral part of the overall California public health emergency preparedness and response strategy where completion and implementation of CalREDIE allows for 24/7/365 reporting and receipt of notifiable conditions. LHDs and CDPH will have access to disease and laboratory reports in near real-time for disease surveillance, public health investigation, and case management activities. CalREDIE is the system of record for communicable disease surveillance data within California.

IV. Legal Authority for Use and Disclosure of Protected Data: The legal authority for CDPH to collect, use and disclose Protected Data, and for Data Recipient to receive and use Protected Data is as follows:

A. General Legal Authority:

1. California Information Practices Act:
   a) California Civil Code section 1798.24, subdivision (e), provides in part as follows: "No agency may disclose any personal information in a manner that would link the information disclosed

to the individual to whom it pertains unless the information is disclosed, as follows:To a person, or to another agency where the transfer is necessary for the transferee agency to perform its constitutional or statutory duties, and the use is compatible with a purpose for which the information was collected..."

B. Specific Legal Authority -- List of Reportable Diseases and Conditions:

1. California Health and Safety Code section 120130 provides in part as follows: "The jurisdiction shall establish a list of reportable diseases and conditions. For each reportable disease and condition, the jurisdiction shall specify the timeliness requirements related to the reporting of each disease and condition, and the mechanisms required for, and the content to be included in, reports made pursuant to this section. The list of reportable diseases and conditions may include both communicable and noncommunicable diseases. Those diseases listed as reportable shall be properly reported as required to the jurisdiction by the health Officer . . . ."
2. California Health and Safety Code section 120130 also provides in part as follows: "Commencing July 1, 2009, or within one year of the establishment of a state electronic laboratory reporting system, whichever is later, a report generated pursuant to [Section 120130] by a laboratory shall be submitted electronically in a manner specified by the jurisdiction, except that this electronic reporting requirement shall not apply to reports of HIV infections . . . ."
3. Title 17 of the California Code of Regulations, section 2500, subdivision (g), provides in part as follows: "Upon the State Department of Public Health's request, a local health jurisdiction shall provide to the Department the information reported pursuant to this section . . . ." Other sections of Title 17 of the California Code of Regulations provide authority for the uses and disclosures that are the subject of this Agreement, including, Sections 2501, 2502, 2593, 2641.5-2643.20, and 2800-2812.

C. Health Insurance Portability and Accountability Act of 1996 (HIPAA) Authority:

1. CDPH HIPAA Status: CDPH is a "hybrid entity" for purposes of applicability of the federal regulations entitled "Standards for Privacy of Individually Identifiable Health Information" ("Privacy Rule") (45 C.F.R. Parts 160, 162, and 164) promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (42 U.S.C. §§ 1320d - 1320d-8) (as amended by Subtitle D Privacy, of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111–5, 123 Stat. 265–66)). None of the CDPH programs that collect, use or disclose Protected Data have been designated by the CDPH as HIPAA-covered "health care components" of CDPH. (45 C.F.R. § 164.504(c)(3)(iii).).
2. Parties Are "Public Health Authorities": CDPH and Data Recipient are each a "public health authority" as that term is defined in the Privacy Rule. (45 C.F.R. §§ 164.501; 164.512(b)(1)(i).)
3. Protected Data Use and Disclosure Permitted by HIPAA: To the extent a disclosure or use of Protected Data is a disclosure or use of "Protected Health Information" (PHI) of an individual, as that term is defined in Section 160.103 of Title 45, Code of Federal Regulations, the following Privacy Rule provisions apply to permit such Protected Data disclosure and/or use by CDPH and Data Recipient, without the consent or authorization of the individual who is the subject of the PHI:
   a) The HIPAA Privacy Rule creates a special rule for a subset of public health disclosures whereby HIPAA cannot preempt state law if, "[t]he provision of state law, including state procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention." (45 C.F.R. § 60.203(c) [HITECH Act, § 13421, sub. (a)].) [NOTE: See State laws and regulations listed in §§ IV.A and IV.B, above.];
   b) A covered entity may disclose PHI to a "public health authority" carrying out public health activities authorized by law; (45 C.F.R. § 164.512(b).); and

c) Other, non-public health-specific provisions of HIPAA may also provide the legal basis for all or specific Protected Data uses and disclosures.

V. Disclosure Restrictions: The Data Recipient and its employees or agents, shall protect from unauthorized disclosure any Protected Data. The Data Recipient shall not disclose, except as otherwise specifically permitted by this Agreement, any Protected Data to anyone other than CDPH, except if disclosure is required by state or federal law.

VI. Use Restrictions: The Data Recipient and its employees or agents, shall not use any Protected Data for any purpose other than carrying out the Data Recipient's obligations under the statutes and regulations set forth in Section IV, above, or as otherwise allowed or required by state or federal law.

VII. Safeguards: Data Recipient shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the privacy, confidentiality, security, integrity, and availability of Protected Data, including electronic or computerized Protected Data. The Data 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 the Data Recipient's operations and the nature and scope of its activities in performing its legal obligations and duties (including performance of its duties and obligations under this Agreement), and which incorporates the requirements of Section VIII, Security, below. Data Recipient shall provide CDPH with Data Recipient's current and updated policies.

VIII. Security: The Data Recipient shall take all steps necessary to ensure the continuous security of all computerized data systems containing Protected Data. These steps shall include, at a minimum:

A. complying with all of the data system security precautions listed in the Data Recipient Data Security Standards set forth in Attachment A to this Agreement;

B. providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III- Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and

In case of a conflict between any of the security standards contained in any of the aforementioned sources of security standards, the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to Protected Data from breaches and security incidents.

IX. Security Officer: The Data Recipient shall designate a Security Officer to oversee its compliance with this Agreement and for communicating with CDPH on matters concerning this Agreement.

X. Training: The Data 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 Data Recipient's obligations under this Agreement, or otherwise use or disclose Protected Data.

A. The Data Recipient shall require each employee who receives training to sign a certification, indicating the employee's name and the date on which the training was completed.

B. The Data Recipient shall retain each employee's written certifications for CDPH inspection for a period of three years following contract termination.

XI. Employee Discipline: Data Recipient shall discipline such employees and other Data Recipient workforce members who intentionally violate any provisions of this Agreement, including, if warranted, by termination of employment.

XII. Breach and Security Incident Responsibilities:

A. Notification to CDPH of Breach or Security Incident: The Data Recipient shall notify CDPH **immediately by telephone call plus email or fax** upon the discovery of a breach (as defined in this Agreement), **or** within **twenty-four (24) hours by email or fax** of the discovery of any security incident (as defined in this Agreement). Notification shall be provided to the CDPH Program Manager, the CDPH Privacy Officer and the CDPH Chief Information Security Officer, using the contact information listed in Section XII(c), below. If the breach or security incident occurs after business hours or on a weekend or holiday and involves Protected Data in electronic or computerized form, notification to CDPH shall be provided by calling the CDPH IIT Service Desk at the telephone numbers listed in Section XII(c), below For purposes of this Section, breaches and security incidents shall be treated as discovered by Data Recipient as of the first day on which such breach or security incident is known to the Data Recipient, or, by exercising reasonable diligence would have been known to the Data Recipient. Data Recipient shall be deemed to have knowledge of a breach or security incident if such breach or security incident is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach or security incident, who is an employee or agent of the Data Recipient.

Data 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 required by applicable federal and state laws, including, specifically, California Civil Code section 1798.29.

B. Investigation of Breach: The Data Recipient shall immediately investigate such breach or security incident, and within seventy-two (72) hours of the discovery, shall inform the CDPH Help Desk, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer of:

1. what data elements were involved and the extent of the data 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 Protected Data and/or a description of the unauthorized persons known or reasonably believed to have improperly accessed or acquired the Protected Data, or to whom it is known or reasonably believe have had the Protected Data improperly disclosed to them; and
3. a description of where the Protected Data is believed to have been improperly used or disclosed; and
4. a description of the probable 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: The Data Recipient shall provide a written report of the investigation to the CDPH Program Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer within five (5) working days of 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 full, 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 of 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 Data Recipient is considered only a custodian and/or non-owner of the Protected Data, Data 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. The CDPH Privacy Officer shall approve 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. CDPH Contact Information: To direct communications to the above referenced CDPH staff, the Data Recipient shall initiate contact as indicated herein. CDPH reserves the right to make changes to the contact information below by giving written notice to the Data Recipient. Said changes shall not require an amendment to this Agreement.

CDPH Program Manager	CDPH Privacy Officer	CDPH Chief Information Security Officer (and CDPH IT Service Desk)
CalREDIE Help Desk California Department of Public Health P.O. Box 997377, MS 7303 Sacramento, CA 95899-7377 California Department of Public Health Email: CalREDIEHelp@cdph.ca.gov Telephone: (866) 866-1428	**Privacy Officer** Privacy Office, c/o Office of Legal Services California Department 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 Department of Public Health P.O. Box 997413, MS 6302 Sacramento, CA 95899-7413 Email: cdphiso@cdph.ca.gov Telephone: IT Service Desk (916) 440-7000 or (800) 579-0874

XIII. Indemnification: Data Recipient shall indemnify, hold harmless and defend CDPH from and against any and all claims, losses, liabilities, damages, costs and other expenses (including attorneys fees) that result from or arise directly or indirectly out of or in connection with any negligent act or omission or willful misconduct of Data Recipient, its officers, employees or agents relative to the Protected Data, including without limitation, any violation~~s~~ of Data Recipient's responsibilities under this Agreement.

XIV. Term of Agreement: This Agreement shall remain in effect for three (3) year after the latest signature date in the signature block below. After three (3) year, this Agreement will expire without further action. If the parties wish to extend this Agreement, they may do so by reviewing, updating, and reauthorizing this Agreement. The newly signed agreement should explicitly supersede this Agreement, which should be referenced by Agreement Number and date in Section I of the new Agreement. If one or both of the parties wish to terminate this Agreement prematurely, they may do so upon 30 days advanced notice. CDPH may also terminate this Agreement pursuant to Sections XV or XVII, below.

XV. Termination for Cause:

A. Termination Upon Breach: A breach by Data 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 the Agreement by CDPH. At its sole discretion, CDPH may give Data Recipient 30 days to cure the breach.

B. Judicial or Administrative Proceedings: Data 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 Data Recipient is found guilty of a criminal violation related to a violation of this Agreement. CDPH may terminate

the Agreement if a finding or stipulation that the Data Recipient has violated any security or privacy laws is made in any administrative or civil proceeding in which the Data Recipient is a party or has been joined.

XVI. Return or Destruction of Protected Data on Expiration or Termination: On expiration or termination of the agreement between Data Recipient and CDPH for any reason, Data Recipient shall return or destroy the Protected Data. If return or destruction is not feasible, Data Recipient shall explain to CDPH why, in writing, to the CDPH Help Desk, the CDPH Privacy Officer and the CDPH Chief Information Security Officer, using the contact information listed in Section XIII(c), above.

A. Retention Required by Law: If Required by state or federal law, Data Recipient may retain, after expiration or termination, Protected Data for the time specified as necessary to comply with the law.

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

C. Notification of Election to Destroy Protected Data: If Data Recipient elects to destroy the Protected Data, Data Recipient shall certify in writing, to the CDPH Program Manager, the CDPH Privacy Officer and the CDPH Chief Information Security Officer, using the contact information listed in Section XIII(c), above. that the Protected Data has been destroyed.

XVII. Amendment: The parties acknowledge that Federal and State laws relating to information security and privacy are rapidly evolving 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 Protected Data. Upon CDPH' request, Data Recipient agrees to promptly enter into negotiations with CDPH concerning an amendment to this Agreement embodying written assurances consistent with new standards and requirements imposed by regulations and other applicable laws. CDPH may terminate this Agreement upon thirty (30) days written notice in the event:

A. Data Recipient does not promptly enter into negotiations to amend this Agreement when requested by CDPH pursuant to this Section or

B. Data Recipient does not enter into an amendment providing assurances regarding the safeguarding of Protected Data that CDPH in its sole discretion deems sufficient to satisfy the standards and requirements of applicable laws and regulations relating to the security or privacy of Protected Data.

XVIII. Assistance in Litigation or Administrative Proceedings: Data Recipient shall make itself and any employees or agents assisting Data Recipient in the performance of its obligations under this Agreement, available to CDPH at no cost to CDPH to testify as witnesses, or otherwise, 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 the Data Recipient, except where Data Recipient or its employee or agent is a named adverse party.

XIX. Disclaimer: CDPH makes no warranty or representation that compliance by Data Recipient with this Agreement will be adequate or satisfactory for Data Recipient's own purposes or that any information in Data Recipient's possession or control, or transmitted or received by Data Recipient, is or will be secure from unauthorized use or disclosure. Data Recipient is solely responsible for all decisions made by Data Recipient regarding the safeguarding of Protected Data.

XX. Transfer of Rights: Data Recipient has no right and shall not subcontract, delegate, assign, or otherwise transfer or delegate any of its rights or obligations under this Agreement to any other person or entity. Any such transfer of rights shall be null and void.

XXI. 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 Data Recipient and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

XXII. Interpretation: The terms and conditions in this Agreement shall be interpreted as broadly as necessary to implement and comply with regulations and applicable State and Federal 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.

XXIII. Survival: The respective rights and obligations of Data Recipient under **Sections VII, VIII and XII** of this Agreement shall survive the termination or expiration of this Agreement .

XXIV. Entire Agreement: This Agreement constitutes the entire agreement between CDPH and Data 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.

XXV. Severability: The invalidity in whole or in part of any provisions of this Agreement shall not void or affect the validity of any other provisions of this Agreement.

XXVI. Signatures:

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

On behalf of the **Data Recipient**, the undersigned individual hereby attests that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.

_____	_____	_____	_____
Name (Print)	**Name (Sign)**	**Title**	**Date**
Health Officer- Humboldt County Health Department			

On behalf of the **Department of Public Health**, the undersigned individual(s) hereby attests that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.

_____ _____

Gilberto F. Chávez, M.D., M.P.H **Date**

the State Epidemiologist – California Department of Public Health

_____ _____

Greg Oliva, M.P.H **Date**

the CalREDIE Product Director – California Department of Public Health

Attachment A

Data Recipient Data Security Standards

1. **General Security Controls**

a) ***Confidentiality Statement.*** All persons that will be working with Protected Data must sign a confidentiality statement. The statement must include at a minimum, General Use, Security and Privacy safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to Protected Data. The statement must be renewed annually. The Data Recipient shall retain each person's written confidentiality statement for CDPH inspection for a period of three (3) years following contract termination.

b) ***Workstation/Laptop encryption.*** All workstations and laptops that process and/or store Protected Data must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher. The encryption solution must be full disk unless approved by the CDPH Information Security Office.

c) ***Server Security.*** Servers containing unencrypted Protected Data must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

d) ***Minimum Necessary.*** Only the minimum necessary amount of Protected Data required to perform necessary business functions may be copied, downloaded, or exported.

e) ***Removable media devices.*** All electronic files that contain Protected Data data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, Blackberry, backup tapes etc.). Must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher

f) ***Antivirus software.*** All workstations, laptops and other systems that process and/or store Protected Data must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

g) ***Patch Management.*** All workstations, laptops and other systems that process and/or store Protected Data must have security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release.

h) ***User IDs and Password Controls.*** All users must be issued a unique user name for accessing Protected Data. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password. Passwords are not to be shared. Must be at least eight characters. Must be a non-dictionary word. Must not be stored in readable format on the computer. Must be changed every 60 days. Must be changed if revealed or compromised. Must be composed of characters from at least three of the following four groups from the standard keyboard:

- Upper case letters (A-Z)
- Lower case letters (a-z)
- Arabic numerals (0-9)
- Non-alphanumeric characters (punctuation symbols)

i) ***Data Sanitization.*** All Protected Data must be sanitized using NIST Special Publication 800-88 standard methods for data sanitization when the CDPH PSCI is no longer needed.

2. **System Security Controls**

a) ***System Timeout.*** The system must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.

b) ***Warning Banners.*** All systems containing Protected Data must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only. User must be directed to log off the system if they do not agree with these requirements.

c) ***System Logging.*** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for Protected Data, or which alters Protected Data. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If Protected Data is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.

d) ***Access Controls.*** The system must use role based access controls for all user authentications, enforcing the principle of least privilege.

e) ***Transmission encryption.*** All data transmissions of Protected Data outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher. Encryption can be end to end at the network level, or the data files containing Protected Data can be encrypted. This requirement pertains to any type of Protected Data in motion such as website access, file transfer, and E-Mail.

f) ***Intrusion Detection***. All systems involved in accessing, holding, transporting, and protecting Protected Data that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

3. **Audit Controls**

a) ***System Security Review.*** All systems processing and/or storing Protected Data must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews shall include vulnerability scanning tools.

b) ***Log Reviews.*** All systems processing and/or storing Protected Data must have a routine procedure in place to review system logs for unauthorized access.

c) ***Change Control.*** All systems processing and/or storing Protected Data must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

4. **Business Continuity / Disaster Recovery Controls**

a) ***Disaster Recovery.*** Data Recipient must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic Protected Data in the event of an emergency. Emergency

means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this agreement for more than 24 hours.

b) ***Data Backup Plan.*** Data Recipient must have established documented procedures to backup Protected Data to maintain retrievable exact copies of Protected Data. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and the amount of time to restore Protected Data should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of CDPH data.

5. **Paper Document Controls**

a) ***Supervision of Data.*** Protected Data in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. Protected Data in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

b) ***Escorting Visitors.*** Visitors to areas where Protected Data is contained shall be escorted and CDPH PHI shall be kept out of sight while visitors are in the area.

c) ***Confidential Destruction.*** Protected Data must be disposed of through confidential means, using NIST Special Publication 800-88 standard methods for data sanitization when the CDPH PSCI is no longer needed.

d) ***Removal of Data.*** Protected Data must not be removed from the premises of the Data Recipient except with express written permission of CDPH.

e) ***Faxing.*** Faxes containing Protected Data shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending.

f) ***Mailing.*** Protected Data shall only be mailed using secure methods. Large volume mailings of CDPH PHI shall be by a secure, bonded courier with signature required on receipt. Disks and other transportable media sent through the mail must be encrypted with a CDPH approved solution, such as a solution using a vendor product specified on the CSSI.