**PRIVACY AND SECURITY REQUIREMENTS**

1. **Purpose of Exhibit**
2. This Exhibit sets forth the privacy and security requirements that apply to all Personally Identifiable Information (PII) that Contractor obtains, maintains, transmits, uses or discloses from Covered California pursuant to this Agreement.
3. The parties agree to all terms and conditions of this Exhibit in order to ensure the integrity, security, and confidentiality of the information exchanged pursuant to this Agreement, and to allow disclosure and use of such information only as permitted by law and only to the extent necessary to perform functions and activities pursuant to this Agreement.
4. This Exhibit establishes requirements in accordance with applicable federal and state privacy and security laws including, but not limited to, the Information Practices Act (California Civil Code Section 1798 et seq.), the federal Patient Protection and Affordable Care Act (P.L. 111-148), as amended by the federal Health Care and Education Reconciliation Act of 2010 (P.L. 111-152) (herein, the “Affordable Care Act”), and its implementing regulations at 45 C.F.R. Sections 155.260 and 155.280 (the “Exchange Privacy and Security Rules”) and, where applicable, the Health Insurance Portability and Accountability Act (42 U.S.C. Section 1320d-d8) and the Health Information Technology for Economic and Clinical Health Act and their implementing regulations at 45 C.F.R. Parts 160 and 164 (collectively, “HIPAA”), as well as applicable privacy and security control protocols set forth within the Minimum Acceptable Risks For State-Based Exchanges document suite (“MARS-E”).
5. **Definitions**

The following definitions shall apply to this Exhibit:

1. Breach: Shall mean a confirmed “breach of the security of the system” as such term is specifically-defined within the CA Information Practices Act [CA Civ. Code §1798.29(f)].
2. Disclosure: The release, transfer, provision of access to, or divulging in any other manner of PII outside the entity holding the information. For purposes of this Exhibit, disclosure includes if a person or entity outside of the entity holding the information takes possession or control of PII, such as if PII is encrypted by an unauthorized person as the result of a ransomware attack.
3. Personal Information or PI: Information that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual [CA Civ. Code §1798.3].
4. Personally Identifiable Information or PII: Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc. (OMB M-07-16.) PII includes Personal Information (PI) and Protected Health Information (PHI).
5. Protected Health Information or PHI: Individually Identifiable Health Information that is transmitted by electronic media, maintained in electronic media, or is transmitted or maintained in any other form or medium, as defined in 45 C.F.R. Section 160.103.
6. Privacy Incident: shall mean either: i) the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII, whether physical, or electronic; or ii) a reasonable belief that unauthorized acquisition of PII that compromises the security, confidentiality or integrity of the PII has occurred
7. Security Incident: The act of violating an explicit or implied security policy, which includes attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent. Incidents include the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, and misrouting of mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification, or destruction. Adverse events such as floods, fires, electrical outages, and excessive heat are not considered incidents. (Computer Matching Agreement, Agreement No. 2013-11, p.5.)
8. **Applicable Laws**

Contractor shall comply with any and all federal and state privacy and security laws, as well as applicable rules and regulations pertaining to Covered California including, but not limited to, those arising under the federal Patient Protection and Affordable Care Act and its implementing regulations. To the extent a conflict arises between any laws or other requirements, Contractor agrees to comply with the applicable requirements imposing the more stringent privacy and security standards.

1. Exchange Privacy and Security Rules (45 C.F.R. Section 155.260).
2. In accessing, collecting, using or disclosing PII in performing functions for Covered California as authorized by this Agreement, Contractor shall only use or disclose PII to the minimum extent such information is necessary to perform such functions.
3. Contractor shall establish and implement privacy and security standards that are consistent with the principles of 45 C.F.R. Section 155.260(a)(3) as set forth below in subsections (i) through (viii):
4. Individual access. Individuals shall be provided with a simple and timely means to access and obtain their PII in a readable form and format;
5. Correction. Individuals shall be provided with a timely means to dispute the accuracy or integrity of their PII and to have erroneous information corrected or to have a dispute documented if their requests are denied;
6. Openness and transparency. Contractor shall be open and transparent regarding its policies, procedures, and technologies that directly affect individuals and/or their PII;
7. Individual choice. Individuals shall be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their PII;
8. Collection, use and disclosure limitations. PII shall be created, collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately;
9. Data quality and integrity. Contractor will take reasonable steps to ensure that PII is complete, accurate, and up-to-date to the extent necessary for Contractor’s intended purposes and has not been altered or destroyed in an unauthorized manner;
10. Safeguards. PII will be protected with reasonable operational, administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure; and,
11. Accountability. Contractor will use appropriate monitoring and other means and methods to assure accountability with these principles and to report and mitigate non-adherence and breaches.
12. California Information Practices Act. Contractor shall comply with the applicable privacy and security provisions of the Information Practices Act of 1977, California Civil Code Section 1798 et seq. and shall provide assistance to Covered California as may be reasonably necessary for Covered California to comply with these provisions [CA Civ. Code §1798].
13. Health Insurance Portability and Accountability Act (“HIPAA”).
14. Contractor expressly acknowledges and agrees that Covered California is not a health care provider, a health care plan, or a health care clearinghouse. Accordingly, the parties mutually acknowledge and agree that, for purposes of this Agreement, Covered California is not a Covered Entity as such term is specifically defined in HIPAA.
15. Contractor expressly acknowledges and agrees that where Covered California performs a function required under applicable law pursuant to 45 C.F.R. Section 155.200, it is not acting as a Business Associate of any other Covered Entity and Contractor is not acting as Covered California’s Business Associate, as such terms are specifically defined in HIPAA. Should Covered California determine Contractor to be a Covered Entity or Business Associate as specifically-defined within HIPAA, Contractor shall at all times comply with applicable privacy and information security obligations imposed under HIPAA pertaining to any PII subject to this Agreement.

1. Fingerprinting and Background Checks. (CA Gov. Code Section 1043).
2. Before any individual who provides services related to this Agreement may access PII, including but not limited to any employee, subcontractor or other person, Contractor must ensure that any such individual shall agree to a criminal background check, which shall be conducted by Covered California in accordance with California Government Code Section 1043, and its implementing regulations set forth in California Code of Regulations, Title 10, Section 6456. Fees charged by the California Department of Justice for the cost of processing such requests shall be paid by Contractor.
3. Background check records shall be maintained by Covered California for so long as any such individual is employed with Contractor or, if applicable, Contractor’s subcontractor plus a period of no less than five (5) years thereafter. Contractor shall provide Covered California with a list of any such individuals subject to this requirement and shall provide, update and notify Covered California of any personnel changes involving any such individuals via e-mail at [backgroundchecks@covered.ca.gov](mailto:backgroundchecks@covered.ca.gov).
4. For any insurance agent licensed by the California Department of Insurance (CDI) Covered California may obtain a criminal history check in accordance with Government Code Section 1043 from CDI.
5. Privacy and Security Awareness Training (MARS-E).
6. Contractor shall ensure that any and all employees, agents, representatives or subcontractors who are provided access to PII have been provided privacy and security awareness training prior to accessing PII.
7. Contractor shall provide annual privacy and security awareness training to the aforementioned individuals no less than once per year thereafter.
8. Contractor shall likewise ensure that any and all such employees, agents, representatives or subcontractors certify in writing their completion of any such privacy and security awareness programs and, upon request, shall provide Covered California with copies of the same.
9. Contractor shall retain the aforementioned certifications for a period of five (5) years and shall provide the copies upon request during this time.
10. Upon reasonable request by Covered California, Contractor shall ensure that the aforementioned individuals subject to the above-referenced training requirements are enrolled in and participate in privacy and security awareness training provided by Covered California. Privacy and security awareness training provided by Covered CA shall be provided in an online format, free-of-charge and, upon reasonable request, Contractor shall cooperate in good-faith with Covered California to ensure that any such individuals are provided access.

1. Notwithstanding the foregoing, Contractor shall be deemed to have complied with the above-referenced requirements through the completion of any certification program which includes privacy and security awareness training and is required for Contractor’s participation in Covered California.
2. **Consumer Rights**
3. Accounting of Disclosures
4. Contractor shall assist Covered California in responding to accounting requests by individuals that are made to Covered California under the Information Practices Act (Civil Code Section 1798.25-29) and if Protected Health Information is involved, pursuant to HIPAA, 45 C.F.R. Section 164.528.
5. The obligation of Contractor to provide an accounting of disclosures as set forth herein survives the expiration or termination of this Agreement with respect to accounting requests made after such expiration or termination.
6. Copies of Records Requests

Regardless of whether a request is made to Covered California or to Contractor, Contractor shall respond to the request with respect to the record Contractor and its subcontractors maintain, if any, in a manner and time frame consistent with requirements specified in the Information Practices Act (Civil Code Sections 1798.30-1798.34) and if Protected Health Information is involved, with HIPAA (45 C.F.R Section 164.524).

1. Requests to Amend Records
2. Contractor shall make any amendments to Personally Identifiable Information in a record that Covered California directs or agrees to, whether at the request of Covered California or an Individual.
3. Regardless of whether a request to amend records is made to Covered California or to Contractor, Contractor shall respond to the request with respect to the record Contractor and its subcontractors maintain in a manner and time frame consistent with requirements specified in the Information Practices Act (Civil Code Section 1798.35) and if Protected Health Information is involved, with HIPAA (45 C.F.R. Section 164.526).
4. Requests to Restrict Use and Disclosure of Personally Identifiable Information
5. Contractor shall reasonably comply with any requests to restrict the use and disclosure of Personally Identifiable Information.
6. If Protected Health Information is involved, Contractor shall respond to the request in a manner and time frame consistent with requirements specified in HIPAA (45 C.F.R. Section 164.522).
7. Confidential Communications Request
8. Upon receipt of written notice, Contractor shall reasonably comply with any requests to utilize an alternate address, email, or telephone number when communicating with the individual.
9. If the request is denied, a written response shall be sent to the individual stating the reasons for denying the request.
10. If Protected Health Information is involved, regardless of whether a request is made to Covered California or to Contractor, Contractor shall respond to the request in a manner and time frame consistent with requirements specified in HIPAA (45 C.F.R. Section 164.522(b)(1)).
11. In responding to any requests from individuals, Contractor shall verify the identity of the person making the request to ensure that the person is the individual who is the subject of the PII or has authority to make requests concerning the PII before responding to the request.
12. In the event any individual submits any of these requests directly from the Contractor, Contractor shall within five (5) calendar days forward such request to Covered California.

**E. General Safeguards and Security Controls**

1. General Safeguards: Contractor shall establish and implement operational, technical, administrative and physical safeguards that are consistent with any applicable laws to ensure:
   1. The confidentiality, integrity, and availability of Personally Identifiable Information created, collected, used, and/or disclosed by the Exchange;
   2. Personally Identifiable Information is only used by or disclosed to those authorized to receive or view it;
   3. Personally Identifiable Information is protected against any reasonably anticipated threats or hazards to the confidentiality, integrity, and availability of such information;
   4. Personally Identifiable Information is protected against any reasonably anticipated uses or disclosures of such information that are not permitted or required by law; and
   5. Personally Identifiable Information is securely destroyed or disposed of in an appropriate and reasonable manner and in accordance with retention schedules.

2. Security Controls:

1. Electronic PII

i) Encryption. Contractor shall encrypt all PII that is in motion or at rest, including but not limited to data on portable media devices, laptops and workstations, with FIPS 140-2 compliant encryption, including but not limited to any PII transmissions which occur via website access, file transfer or e-mail. Encryption protocols implemented by Contractor shall at all times be consistent with the National Institute for Standards and Technology (“NIST”) security controls concerning the protection of PII. The aforementioned encryption requirement shall at all times be applicable to PII transmissions both within and outside of Covered California’s secure internal network and may be fulfilled either through network-level end-to-end encryption or the encryption of any data files containing PII.

ii) Hardware. Contractor shall ensure that any and all hardware, including but not limited to personal computers, laptops, jump-drives, smart phones or other devices upon which PII is stored, is secured, password-protected and only accessible by Contractor or Contractor’s agents, employees or sub-contractors in accordance with the terms of this Agreement. Contractor shall at all times remove and permanently delete any and all PII before any such hardware is transferred or sold to a third-party or is otherwise subject to any change in ownership or control.

iii) Log-In Credentials. Contractor shall at all times ensure that each individual user of any Exchange computer system through which PII is accessed maintains his or her own unique user-id and password. Contractor shall strictly refrain from sharing individual log-in credentials and shall at all times assume responsibility for ensuring that the log-in credentials of any former employees, sub-contractors, agents or other representatives who are no longer subject to this Agreement are de-activated or otherwise changed to prevent unauthorized access by any such individuals within 24 hours.

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

v) Minimum Necessary. Only the minimum necessary amount of PII required to perform necessary business functions may be copied, downloaded, or exported.

vi) Data Destruction. When no longer needed, all PII must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the PSCI cannot be retrieved.

vii) Access Controls. The system providing access to PII must use role based access controls for all user authentications, enforcing the principle of least privilege.

b. Paper-Based PII:

1. Supervision of Data. PII 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. PII 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.
2. Escorting Visitors. Visitors to areas where PII is contained shall be escorted and PII shall be kept out of sight while visitors are in the area.

iii) Confidential Destruction. PII must be disposed of through confidential means, such as cross cut shredding and pulverizing in accordance with Covered California secure document destruction protocols.

iv) Removal of Data. PII must not be removed from the premises of the Contractor except with express written permission of the Exchange.

v) Faxing. Faxes containing PII 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 the fax.

vi) Mailing. Mailings of PII shall be sealed and secured from damage or inappropriate viewing of PII to the extent possible. Mailings which include 500 or more individually identifiable records of PII in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of the Covered California to use another method is obtained.

**F. Single Point of Contact**

* + - 1. Contractor shall designate one (1) individual to serve as the single point of contact (“SPOC”) in matters pertaining to Contractor’s information security and privacy program and the implementation of the requirements set forth herein. The name and contract information of the aforementioned SPOC shall be submitted to the Covered California Information Security and Privacy Offices via e-mail at, respectively:

[informationsecurity@covered.ca.gov](mailto:informationsecurity@covered.ca.gov); and

[privacyofficer@covered.ca.gov](mailto:privacyofficer@covered.ca.gov)

no later than sixty (60) days following the Effective Date of this Agreement.

1. The SPOC may, in his or her discretion, delegate project-related tasks to other individuals but shall at all times remain responsible for ensuring compliance with the security and privacy-related requirements specified within this Agreement and for communicating with the Covered California Information Security and Privacy Offices in security and privacy-related matters.
2. To ensure compliance with Exchange security and privacy standards specified herein, Contractor’s SPOC shall complete and submit a copy of the Covered California Annual Security and Privacy Attestation (“SPA”) attached and incorporated herein by reference as Attachment 1. Contractor’s Annual SPA shall be due no later than one (1) year following the Effective date of this Agreement, then annually thereafter.

**G. Policies and Procedures**

1. Contractor shall implement and maintain written policies and procedures to ensure the privacy and security of PII stored, maintained, or accessed in compliance with this agreement and any applicable laws. Such policies shall address:
   1. The implementation of consumer rights as required by this Exhibit;
   2. Reasonable safeguards as required by this Exhibit;
   3. Contractor’s processes for monitoring, periodically assessing, and updating security controls to ensure the continued effectiveness of those controls; and
   4. The training of Contractor’s employees, agents and subcontractors.
2. Upon request, Contractor shall provide Covered California with copies of any such policies and procedures adopted by Contractor to meet its obligations under this Agreement. Should Covered California determine any such policies and procedures to be insufficient, Contractor agrees to cooperate in good faith to incorporate appropriate revisions required by Covered California to bring any such policies and procedures into compliance.
3. Contractor agrees to apply appropriate sanctions against any of its workforce members who fail to comply with its privacy policies and procedures or the provisions specified herein.

**H. Subcontractors**

1. Contractor shall be bound by and be responsible for the acts and omissions of its subcontractors, agents or vendors in the exchange of data with the Exchange. Contractor shall take reasonable steps to ensure compliance with the terms of this Agreement by any such individuals.
2. Contractor agrees to enter into written contracts with its agents and contractors that obligate such agents or subcontractors to abide by the same privacy and security standards and obligations that Contractor has agreed to in this Agreement.
3. Upon reasonable request by Covered California, Contractor shall provide copies of any written agreements or contracts entered into between Contractor and its agents or subcontractors to fulfill the privacy and security-related obligations specified herein.

**I. Privacy & Security Incidents; Breaches**

* + - 1. Contractor shall immediately report to the Covered California Privacy Officer at [PrivacyOfficer@covered.ca.gov](mailto:PrivacyOfficer@covered.ca.gov) any actual or suspected Privacy or Security Incidents involving PII created or received under this Agreement. Contractor’s report (“Initial Report”) shall be provided on that certain Privacy & Incident Intake Form, developed by the Covered California Privacy Office and attached and incorporated by reference herein as Attachment 2. Contractor’s Initial Report shall, to the maximum extent possible, include the following information to the extent it is known at that time:

1. A brief description of what happened including the date of the incident and the date of the discovery of the incident;
2. The names or identification numbers of the individuals whose PII has been, or is reasonably believed to have been accessed, acquired, used or disclosed
3. A description of the types of PII that were involved in the incident, as applicable;
4. Information regarding any information system intrusion and any systems potentially compromised; and
5. Any other information necessary for Covered California to conduct an investigation and include in notifications to the individual(s) or relevant regulatory authorities under applicable privacy and security requirements.
   * + 1. Following the submission of its Initial Report, Contractor shall immediately commence an investigation in accordance with applicable law to:
6. Determine the scope of the incident;
7. Mitigate harm that may result from the incident; and
8. Restore the security of the system to prevent any further harm or incidents.
   * + 1. Contractor shall cooperate with Covered California in investigating the actual or suspected incident and in meeting Covered California’s obligations, if any, under applicable laws. This includes providing ongoing updates regarding Contractor’s investigation, mitigation, and remediation efforts as more information becomes available or as reasonably requested by Covered California.
9. Unless an extension is granted by Covered California, Contractor will prepare and submit a follow-up report (“Final Report”) within 15 days of submitting its Initial Report. Contractor’s Final Report shall be submitted to the Covered California Privacy Office on the same Privacy & Security Incident Intake Form used for the submission of Covered California’s Initial Report
10. Within its Final Report, Contractor shall describe the results of its investigation, as well as any facts uncovered through the same. Contractor shall make any and all reasonable efforts to obtain the information requested within the Privacy & Security Incident Intake Form and shall provide an explanation if any information requested cannot be obtained.
11. Contractor’s Final Report shall likewise include a corrective action plan which describes the steps to be taken to prevent any future reoccurrence of the incident.
12. Contractor shall cooperate with Covered California in developing content for any public statements and shall not give any public statements regarding any Privacy or Security Incident involving Covered California enrollees without the express written permission of Covered California.
13. If the Privacy Incident is determined to have resulted in a Breach attributable to Contractor or its agents or subcontractors, Contractor shall:
14. Be fully responsible for providing breach notifications to consumers as required under applicable laws;
15. Pay any costs associated with any such Breach notifications as well as any costs or damages associated with the incident; and
16. Should Covered California in its sole discretion determine that credit monitoring is an appropriate remedy, arrange for and bear the reasonable, out-of-pocket cost of providing to each such affected individual one (1) year of credit monitoring services from a nationally recognized supplier of such services.
17. If Contractor determines that a Privacy Incident has not resulted in a Breach, it shall document its assessment and provide such documentation to Covered California within one week of completing its final report. Notwithstanding the foregoing, Covered California reserves the right to reject Contractor’s assessment and direct Contractor to treat the incident as a Breach.

**J. Risk Classification & Assessment**

* + - 1. Covered California may, in its discretion, assign a tier-based risk classification to the disclosure of PII to Contractor under this Agreement.
      2. Determinations as to Contractor’s risk-classification tier shall be made by Covered CA in its sole discretion and Contractor shall be notified of Contractor’s risk-classification prior to the execution of this Agreement and during this Agreement if it changes. Contractor’s risk-classification tier shall be provided to the SPOC appointed by Contractor within Para. F above.
      3. Based on the applicable risk-classification, Contractor acknowledges and agrees that Covered California may impose additional privacy and information security-related obligations, which may include but need not be limited to an annual attestations or annual security assessments.
      4. Contractor shall at all times cooperate in good faith with Covered California in the provision of any information needed by Covered California to ascertain Contractor’s risk classification or the above-referenced security-related documentation.

**K. Right to Inspect**

Covered California may inspect the facilities, systems, books, and records of Contractor to monitor compliance with this Exhibit at any time. Contractor shall promptly remedy any violation reported to it by Covered California and shall certify the same to the Covered California Privacy Officer in writing. The fact that Covered California inspects, fails to inspect, fails to detect violations of this Exhibit or detects but fails to notify Contractor of the violation or require remediation is not a waiver of Covered California’s rights under this Agreement and this Exhibit.

**L. Indemnification**

Contractor agrees to indemnify, defend, and save harmless Covered California, its officers, trustees, agents, and employees from any and all claims, losses, costs, liabilities, damages, and deficiencies, including interest, penalties, attorneys’ fees, breach notification costs to affected individuals, costs for appropriate identity theft prevention and mitigation services, costs for a call center to the extent necessary to respond to affected individuals, costs for restoration of services, costs to retain an alternative contractor where necessary to maintain the availability of services, and any other costs Covered California determines to be reasonable, which arise out of or are due to, or are alleged to arise out of or due to, any of the following:

1. Contractor’s or its subcontractor’s or agent’s failure to comply with the requirements of this Agreement which results in a Breach, as defined in this Exhibit.
2. Use or disclosure of PII by Contractor or its subcontractors or agents that is not permitted by this Agreement.
3. Contractor’s or its subcontractor’s or agent’s failure to comply with the requirements of this Agreement which results in a Security Incident, as defined in this Exhibit.

If Contractor or its subcontractor or agent publishes or discloses PII in violation of this Agreement, Covered California shall additionally be entitled to injunctive relief, or any other remedies to which it is entitled under law or equity, without posting a bond.

The above-referenced indemnification shall be subject to the indemnification procedural requirements set forth in Section E of Exhibit C.

**M. Termination of Agreement**

1. If Contractor breaches its obligations under this Exhibit as determined by Covered California, Covered California may, at its option:
2. Require Contractor to submit to a plan of monitoring and reporting, as Covered California may deem necessary to maintain compliance with this Agreement;
3. Provide Contractor with an opportunity to cure the breach; or
4. After giving Contractor an opportunity to cure the breach, or upon breach of a material term of this Exhibit, terminate this Agreement for cause.
5. A failure of Covered California to exercise any of these options shall not constitute a waiver of its rights under this Agreement.
6. Upon completion of this Agreement, or upon termination of this Agreement, at Covered California’s direction Contractor shall either return all PII to Covered California, or shall destroy all PII in a manner consistent with applicable State and Federal laws, regulations, and agency guidance on the destruction of PII. If return or destruction of PII is not feasible, Contractor shall explain in writing to the Covered California’s Chief Privacy Officer why return or destruction is not feasible. The obligations of Contractor under this Agreement to protect PII and to limit its use or disclosure shall continue and shall survive until all PII is either returned to Covered California or destroyed.