Data Protection Information and Resources

At Everlaw, we are committed to your privacy and to the protection of your personal information. Please take a moment to carefully review our privacy agreements and related documentation. You can find our data privacy addendums for both the California Consumer Privacy Act (CCPA) and the EU General Data Protection Regulation (GDPR) below as well as a comprehensive list of the subprocessors that we partner with to provide services.

For customers who are subject to the requirements of the Health Insurance Portability and Accountability Act (HIPAA), Everlaw can help support your compliance. Customers are responsible for determining whether they use or intend to use Everlaw services in connection with Protected Health Information (PHI). If you wish to use Everlaw with PHI, you must sign a Business Associate Agreement (BAA). For your convenience, we have provided ours below to support your respective HIPAA obligations when using our services.

Customer Data Processing Addendum

This Data Processing Addendum ("**DPA**") is incorporated into and forms part of the Customer Terms of Service found at https://www.everlaw.com/legal/terms, unless the Customer has entered into a superseding written master agreement with Everlaw for the purchase of the Everlaw Service, in which case it forms part of such written agreement (in either case, the "**Agreement**").

This DPA reflects the parties' agreement with regard to the processing by Everlaw of Customer Data on behalf of Customer in connection with the Service, where such Customer Data (defined below) is protected by Data Protection Laws. For any other data, including any admin account information, this DPA shall not apply.

All capitalized terms not defined in this DPA, shall have the meanings set forth in the Agreement. For the avoidance of doubt, all references to

"**Agreement**" shall include this DPA (including, where applicable, the Standard Contractual Clauses).

Customer acknowledges and agrees that it enters into this DPA (including, where applicable, the Standard Contractual Clauses) on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Affiliates and End Clients who are controllers of the Customer Data and permitted to use the Service as "**Authorized Users**" pursuant to the Agreement (each for the purposes of this DPA, an "**Authorized Controller**") and provided that such Authorized Controllers have not entered into their own separate "**Agreement**" as a "**Customer**" with Everlaw. For the purposes of this DPA only, and except where indicated otherwise or the context otherwise requires, the term "**Customer**" shall include Customer and such Authorized Controllers.

The parties agree as follows:

1. **Definitions**
    1. **"Affiliate"** means any entity that is directly or indirectly controlled by, controlling or under common control with an entity. "Control" for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.
    2. **"Customer Data"** means any information that is protected as "personal data" under applicable Data Protection Laws and submitted as Case Materials or are otherwise provided to Everlaw by Customer or its Authorized Users via the Service under the Customer's account.
    3. **"Data Protection Law(s)"** means all data protection laws and regulations of Europe applicable to a party and its processing of Customer Data, including (but not limited to) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("GDPR") and any applicable national implementations of the GDPR.
    4. **"End Clients"** means the Customer's own clients authorized to access the Service under the Customer's account.
    5. **"Europe"** means, for the purposes of this Addendum, the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom.
    6. **"Security Incident"** means any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data

transmitted, stored or otherwise processed by Everlaw and/or its Sub-processor's in connection with the provision of the Service. "Security Incident" shall not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful login attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

7. **"Standard Contractual Clauses"** means the standard contractual clauses for processors as approved by the European Commission pursuant to Commission Decision 2010/87/EC and located here: 32010D0087 – EN – EUR-Lex (or such successor URL).
8. **"Sub-processor"** means any processor engaged by Everlaw to assist in fulfilling its obligations with respect to providing the Service pursuant to the Agreement or this DPA. Sub-processors may include third parties or any Everlaw Affiliates but shall exclude any Everlaw employee, contractor, or consultant.
9. The terms **"controller"**, **"data subjects"**, **"personal data"**, **"processor"** and **"processing"**, **"special category data"** shall have the meaning given to them in Data Protection Law and **"process"**, **"processes"** and **"processed"** shall be interpreted accordingly.

2. **Scope and Applicability of this DPA**
    1. **Scope.** This DPA applies to the extent that Everlaw processes on behalf of Customer any Customer Data protected by Data Protection Laws.
    2. **Role of the parties.** The parties acknowledge and agree that for the purposes of this DPA, Customer is the controller (whether itself a controller or acting on behalf of a third party controller) with respect to the processing of Customer Data, and Everlaw shall process Customer Data only as a processor on behalf of Customer, as further described in Annex A of this DPA. Any processing by either party of personal data under or in connection with the Agreement shall be performed in accordance with applicable Data Protection Laws.
    3. **Processing instructions.** As a processor, Everlaw shall process Customer Data only for the limited purposes described in this DPA and in accordance with Customer's documented lawful instructions. The parties agree that the Agreement (including this DPA and any Order Forms under the Agreement) sets out the Customer's complete and final instructions to Everlaw in relation to the processing of Customer Data and processing outside the scope of these instructions (if any) shall require

prior written agreement between Customer and Everlaw. Without prejudice to Section 2.4 (Customer responsibilities), Everlaw shall notify Customer in writing, unless prohibited from doing so under Data Protection Laws, if it becomes aware or believes that any processing instructions from Customer violate applicable Data Protection Laws.

4. **Customer responsibilities.**
    1. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Data and the means by which Customer acquired Customer Data. Without prejudice to the generality of the foregoing, Customer represents and warrants that (i) it has provided, and will continue to provide all notices and has obtained, and will continue to obtain, all consents, permissions, and rights necessary under applicable laws, including Data Protection Laws, for Everlaw to lawfully process Customer Data for the purposes contemplated by the Agreement (including this DPA and any Order Forms under the Agreement); (ii) it has complied with all applicable laws, including Data Protection Laws in the collection and provision to Everlaw and its Sub-processors of such Customer Data; and (iii) it shall ensure its processing instructions comply with applicable laws (including Data Protection Laws) and that the processing of Customer Data by Everlaw in accordance with Customer's instructions will not cause Everlaw to be in breach of applicable Data Protection Laws.
    2. If Customer is entering into this DPA on behalf of a third party controller (including any Authorized Controller), Customer represents and warrants to Everlaw that Customer's instructions and actions with respect to that Customer Data, including its appointment of Everlaw as a processor or any consents or permissions provided under this DPA with respect to the processing of Customer Data, have been authorized by the relevant controller.

3. **Subprocessing**
    1. **Authorized Sub-processors.** Customer agrees that Everlaw may engage Sub-processors to process Customer Data on Customer's behalf. A current list of Sub-processor's engaged by Everlaw is accessible via https://www.everlaw.com/legal/data-protection/DPA/subprocessors (or such successor URL as may be designated by Everlaw). Everlaw shall notify Customer if it

adds or replaces any Sub-processors prior to any such changes if Customer subscribes to such notifications by sending an email to privacy@everlaw.com with the subject line "Subprocessor Notification Request" (or by other means established by Everlaw and communicated to Customer from time to time).

2. **Sub-processors Obligations.** Everlaw shall: (i) enter into a written agreement with each Sub-processor containing data protection terms that provide at least the same level of protection for Customer Data as those contained in this DPA, to the extent applicable to the nature of the services provide by such Sub-processor; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause Everlaw to breach any of its obligations under this DPA.
3. **Objection to Sub-processors.** Customer may object in writing to Everlaw's appointment of a new Sub-processor on reasonable grounds relating to data protection (e.g. if making Customer Data available to the Sub-processor may violate applicable Data Protection Laws) by notifying Everlaw promptly in writing within fifteen (15) calendar days of receipt of Everlaw notice in accordance with Section 3.Such notice shall explain the reasonable grounds for the objection and the parties shall discuss such concerns in good faith with a view to achieving commercially reasonable resolution. If no such resolution can be reached, Everlaw will, at its sole discretion, either not appoint that proposed Sub-processor, or permit Customer in writing to suspend or terminate the affected Service in accordance with the termination provisions in the Agreement without liability to either party (but without prejudice to any fees incurred by Customer prior to suspension or termination).

4. Security
    1. **Security Measures.** Everlaw shall implement and maintain appropriate technical and organizational security measures designed to protect Customer Data from Security Incidents and to preserve the security and confidentiality of the Customer Data, in accordance with the security standards described in Annex B ("Security Measures"). Everlaw shall ensure that any person who is authorized by Everlaw to process Customer Data shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).
    2. **Security Incident Response.** Upon becoming aware of a Security Incident, Everlaw shall notify Customer without undue

delay and shall: (i) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer; and (ii) promptly take steps, deemed necessary and reasonable by Everlaw, to contain, investigate, and remediate any Security Incident, to the extent that the remediation is within Everlaw's reasonable control. Everlaw's notification of or response to a Security Incident under this Section 4.2 shall not be construed as an acknowledgment by Everlaw of any fault or liability with respect to the Security Incident. The obligations set forth herein shall not apply to Security Incidents to the extent they are caused by Customer or its Authorized Users.

3. **Updates to Security Measures.** Customer acknowledges that the Security Measures are subject to technical progress and development and that Everlaw may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the material degradation of the overall security of the Service purchased by the Customer.
4. **Customer Responsibilities.** Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Service, including securing its account authentication credentials, protecting the security of Customer Data when in transit to and from the Service and taking any appropriate steps to securely encrypt or backup any Customer Data processed in connection with the Service.

5. **Security Audits**
    1. **Audit rights.** Everlaw shall make available to Customer all information reasonably necessary to demonstrate compliance with this DPA and allow for and contribute to audits, including inspections by Customer in order to assess compliance with this DPA. Customer acknowledges and agrees that it shall exercise its audit rights under this DPA (including this Section 4.1 and where applicable, the Standard Contractual Clause) and any audit rights granted by Data Protection Laws, by instructing Everlaw to comply with the audit measures described in Section 5.2.
    2. **Security reports.** Upon written request and a confidential basis, Everlaw shall supply a summary copy of its most current Service Organization Control (SOC) 2 Report (or a comparable report) ("Report") to Customer, so that Customer can verify Everlaw's compliance with this DPA. In addition to the Report,

Everlaw shall (at the Customer's cost and expense) respond to all reasonable requests for information made by Customer to confirm Everlaw's compliance with this DPA, including responses to information security, due diligence, and audit questionnaires, by making additional information available regarding its information security program upon Customer's written request to privacy@everlaw.com, provided that Customer shall not exercise this right more than once per calendar year.

6. **International Transfers**
    1. Customer may choose to have their Customer Data stored and principally processed within Everlaw's available AWS instance(s) located in Europe. Notwithstanding the foregoing, Customer acknowledges that Everlaw may in connection with the performance of the Service (for example, to support, secure, and maintain the Service), need to transfer and process Customer Data to and in the United States and anywhere else in the world where Everlaw or its Sub-processors maintain data processing operations. Everlaw shall at all times ensure such transfers are made in compliance with the requirements of Data Protection Laws and this DPA.
    2. Standard Contractual Clauses. Where Everlaw is a recipient of Customer Data protected by EU Data Protection Laws in the United States or any other third country not recognized as providing adequate protection for personal data (as described in Data Protection Laws), Everlaw agrees to abide by and process such Customer Data in compliance with the Standard Contractual Clauses. For the purposes of the descriptions in the Standard Contractual Clauses, Everlaw agrees that it is a "data importer" and Customer and each Authorized Controller are collectively the "data exporter". It is not the intention of either party, nor the effect of this DPA, to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses. Accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA, the Standard Contractual Clauses shall prevail to the extent of such conflict.
7. **Deletion of Customer Data**
    1. **Deletion on termination.** Upon termination or expiry of the Agreement, on Customer's request Everlaw shall return or delete all Customer Data (including copies) in its possession or control in accordance with the Agreement, save that this requirement shall not apply to the extent Everlaw is required by applicable law to retain some or all of the Customer Data.

8. **Rights of Data Subjects and Cooperation**
    1. **Data Subject Request.** To the extent Customer is unable to independently retrieve, access or delete the relevant Customer Data within the Service, Everlaw shall (at Customer's cost and taking into account the nature of the processing), provide all reasonable cooperation at Customer's request to assist Customer by appropriate technical and organisational measures, in so far as is possible, to respond to any requests from individuals or applicable data protection authorities relating to the processing of Customer Data under the Agreement. In the event that any such request is made to Everlaw directly, Everlaw shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If Everlaw is required to respond to such a request, Everlaw shall promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.
    2. **Subpoenas and Court Orders.** If a law enforcement agency sends Everlaw a demand for Customer Data (for example, through a subpoena or court order), Everlaw shall give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Everlaw is legally prohibited from doing so.
    3. **Data Protection Impact Assessment.** To the extent Everlaw is required under EU Data Protection Law, Everlaw shall provide reasonably requested information regarding Everlaw processing of Customer Data under the Agreement, to the extent Customer does not otherwise have access to the relevant information and to the extent that such information is available to Everlaw, to enable the Customer to carry out data protection impact assessments or prior consultations with supervisory authorities as required by law.
9. **Authorized Controllers**
    1. The parties acknowledge and agree that each Authorized Controller agrees to be bound by the obligations under this DPA, and to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Controller is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Service by Authorized Controllers must comply with the terms and conditions of the Agreement (as they relate to Authorized Users) and any violation of the terms and conditions of the Agreement by an Authorized Controller shall be deemed a violation by the

Customer.

2. The Customer that is the contracting party to the Agreement shall remain responsible for coordinating communications with Everlaw under this DPA and be entitled to make and receive communications in relation to this DPA on behalf of the Authorized Controller.
3. Each Authorized Controller shall, to the extent required under applicable Data Protection Laws, be entitled to exercise the rights and remedies under this DPA, provided that except where applicable Data Protection Laws require the Authorized Controller to exercise a right or seek a remedy under this DPA against Everlaw directly by itself, the parties agree that: (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Controller; and (ii) Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Controller individually but in a combined manner for itself and all Authorized Controllers' together.

10. **Limitation of Liability**
    1. Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA (including the Standard Contractual Clauses) whether in contract, tort (including negligence) or under any other theory of liability, shall be subject to the limitations and exclusions of liability in the Agreement, and any reference in provisions to the liability of a party means the aggregate liability of that party and all of its Affiliates under and in connection with the Agreement and this DPA together.
    2. For the avoidance of doubt, Everlaw's total aggregate liability for all claims from Customer and all Authorized Controller's arising out of or related to the Agreement and this DPA (including the Standard Contractual Clauses), whether in contract, tort (including negligence), or under any other theory of liability, shall apply in aggregate for all claims arising under or in connection with both the Agreement and this DPA, including by Customer and all Authorized Controllers, an in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorized Controller that is a party to this DPA.
11. **Miscellaneous**
    1. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any

conflict between this DPA and the main body of the Agreement, this DPA shall prevail to the extent of that conflict.

2. This DPA shall be deemed a part of and incorporated into the Agreement so that references in the Agreement to "Agreement" shall be interpreted to include this DPA, unless the context requires otherwise.
3. This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by Data Protection Laws.

Annex A – Details of Processing

1. Duration: The duration of the Agreement plus the period from the expiry of the Agreement until the deletion of the Customer Data by Everlaw in accordance with the Agreement.
2. Categories of data subjects: Data subjects include individuals about whom data is provided to Everlaw via the Service (by or a third party acting on behalf of) Customer, which may include, but is not limited to, personal data relating to individuals whose information is included in the Customer Data.
3. Categories of data: Customer (or third parties acting on their behalf) may submit Customer Data to Everlaw in connection with the performance of the Service, the extent of which is exclusively determined and controlled by the Customer.
4. Special categories of data (if appropriate): Customer (or third parties acting on their behalf) may submit Customer Data that contains special categories of data to Everlaw in connection with the performance of the Service, the extent of which is exclusively determined and controlled by the Customer.
5. Nature and Purposes of Processing: (i) Processing to provide the Service in accordance with the Agreement; (ii) processing to perform any steps necessary for the performance of the Agreement; (iii) processing to comply with other reasonable instructions provided by Customer (e.g. via email) that are consistent with the terms of this Agreement (individually and collectively, the "Purpose").
6. Processing operations: Customer Data transferred will be processed in accordance with the Agreement (including this DPA) and may be subject to the following processing activities: (i) storage and other processing necessary to provide, maintain and improve the Service (as applicable) provided to Customer, including analytical capabilities native to the Everlaw platform, data analysis for the purposes of diagnosing support requests and debugging platform issues, and where appropriate the

resolution and reporting on the support requests; and/or (ii) disclosures in accordance with the Agreement and/or as compelled by applicable laws.

Annex B – Security Measures

Everlaw has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security policies and procedures designed to protect Customer Data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction, which at a minimum shall include the measures further summarized and described below. Everlaw regularly monitors compliance with these safeguards. Everlaw will not materially decrease the overall security of the Service during the Term.

1. **Personnel.** Everlaw's personnel will not process Customer Data without authorization. Personnel are legally obligated to maintain the confidentiality of any Customer Data and this obligation continues even after their employment ends.
2. **Data Privacy Contact.**
    1. Everlaw, Inc.
       Attn: Lisa Hawke, Vice President, Security and Compliance
       2101 Webster Street, Suite 1500
       Oakland, CA 94612 USA.
3. **Organization of Information Security.**
    1. *Security Roles and Responsibilities.* Everlaw has appointed Lisa Hawke as the security officer responsible for coordinating and monitoring the security rules and procedures.
    2. *Duty of Confidentiality.* Everlaw's personnel with access to Customer Data are subject to confidentiality obligations via an Everlaw Confidentiality Agreement, Code of Conduct, and supporting policies and procedures.
4. **Risk Management.** Everlaw conducts regular risk assessments and testing and monitoring of the effectiveness of its safeguards, controls, and systems, including conducting vulnerability scanning and penetration testing. The Everlaw Security Management Team ("SMT") implements measures, as needed, to address vulnerabilities discovered in a timely manner.
5. **Storage.** Everlaw's database servers are hosted in a data center operated by a third party vendor, Amazon Web Services ("AWS"), that has been qualified per Everlaw's vendor management procedure. Everlaw maintains complete administrative control over the virtual servers, and no third-party vendors have logical access to Customer Data.

6. **Asset Management.**
    1. *Asset Inventory.* Everlaw maintains an inventory of all media on which Customer Data is stored. Access to the inventories of such media is restricted to authorized personnel.
    2. *Asset Handling.*
        1. Employees are required to utilize encryption to store data in a secure manner and are required to use two-factor authentication to access Everlaw.
        2. Everlaw imposes restrictions handling Customer Data and has procedures for disposing of materials that contain Customer Data.
        3. Everlaw's personnel must obtain authorization prior to storing Customer Data on portable devices and remotely accessing Customer Data.
7. **Software Development and Acquisition.** For the software developed by Everlaw, Everlaw follows secure coding standards and procedures set out in its standard operating procedures.
8. **Change Management.** Everlaw implements documented change management procedures that provide a consistent approach for controlling, implementing, and documenting changes (including emergency changes) to Everlaw's software, information systems or network architecture. These change management procedures include appropriate segregation of duties.
9. **Third-Party Provider Management.** In selecting third party providers who may gain access to, store, transmit or use Customer Data, Everlaw conducts a quality and security assessment pursuant to the provisions of its standard operating procedures.
10. **Human Resources Security.** Everlaw informs its personnel about relevant security and privacy procedures and their respective roles through multiple levels of information security, privacy and security awareness training, as well as of possible consequences of breaching the security rules and procedures. Such consequences include disciplinary and/or legal action.
11. **Physical and Environmental Security.**
    1. *Physical Access to Facilities.* Everlaw limits access to its facility to identified authorized individuals who require such access for the performance of their job function. Everlaw terminates the physical access of individuals promptly following the date of the termination of their employment or services or their transfer to a role no longer requiring access to Customer Data.
    2. *Physical Access to Components.* Everlaw maintains records of the incoming and outgoing physical media containing Customer Data for non-European clients, including the kind of

media, the authorized sender/recipients, date and time, the number of media and the types of Customer Data they contain.

3. *Protection from Disruptions.* Everlaw uses commercially reasonable systems and measures to protect against loss of data due to power supply failure or line interference.
4. *Component Disposal.* Everlaw uses commercially reasonable processes to securely destroy physical media in accordance with the Agreement.

12. **Communications and Operations Management.**
    1. *Security Documents.* Everlaw maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel. These include a suite of information security policies and procedures, security training documents, penetration and vulnerability scanning reports, and SOC 2 (or comparable) security audit reports.
    2. *Data Recovery Procedures.*
        1. On an ongoing basis, Everlaw maintains a copy of Customer Data, which can be recovered. Everlaw has procedures in place governing access to copies of Customer Data and anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data.
        2. The Everlaw Engineering team in cooperation with the Security Management Team is responsible for the development and implementation of backup procedures that are consistent with Everlaw's operations.
        3. Everlaw's cloud services run on AWS, which is designed to deliver 99.999999999% durability, and Everlaw relies on the AWS SLA for this service.
    3. *Encryption; Mobile Media.* Everlaw encrypts data in motion and at rest. Everlaw restricts access to Customer Data in physical media leaving its facilities.
    4. *Event Logging.* Everlaw logs the use of our data-processing systems and maintain logs for at least 10 days.
13. **Access Control.**
    1. *Records of Access Rights.* Everlaw maintains a record of security privileges of individuals having access to Customer Data.
    2. *Access Authorization.*
        1. Everlaw maintains and updates a record of personnel authorized to access systems that contain Customer Data.

2. Everlaw deactivates authentication credentials of employees immediately upon the termination of their employment.
3. Everlaw identifies those personnel who may grant, alter or cancel authorized access to data and resources.

3. *Least Privilege.*
    1. Technical support personnel are only permitted to have access to Customer Data when needed for the performance of their job function.
    2. Everlaw restricts access to Customer Data to only those individuals who require such access to perform their job function.
4. *Integrity and Confidentiality.*
    1. Everlaw instructs its personnel to disable administrative sessions when leaving the Everlaw's premises or when computers are unattended.
    2. Everlaw stores passwords in a way that makes them unintelligible while they are in force.
5. *Authentication.*
    1. Everlaw uses commercially reasonable practices to identify and authenticate users who attempt to access information systems.
    2. Where authentication mechanisms are based on passwords, Everlaw requires the password to be at least eight characters long for Customers and twelve characters long for employees.
    3. Everlaw maintains commercially reasonable procedures to deactivate passwords that have been corrupted or inadvertently disclosed or pursuant to a number of failed login attempts.
    4. Everlaw uses commercially reasonable password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.
6. *Network Design.* Everlaw has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data they are not authorized to access.

14. **Network Security.**
    1. *Network Security Controls.* Everlaw's information systems have security controls designed to detect and mitigate attacks by using logs and alerting.
    2. *Antivirus.* Everlaw implements endpoint protection on its

hosting environments, including antivirus; which are continuously updated with critical patches or security releases in accordance with Everlaw's server change control procedures.

15. **Information Security Incident Management.**
    1. *Record of Breaches.* Everlaw maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.
    2. *Record of Disclosure.* Everlaw tracks disclosures of Customer Data, including what data has been disclosed, to whom, and at what time.
16. **Business Continuity Management.**
    1. *Recovery.* Everlaw employs redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data in its original state from before the time it was lost or destroyed.
    2. *Testing.* Everlaw conducts annual tests of its Business Continuity and Disaster Recovery Procedure.

Annex C – Standard Contractual Clauses (Processors)

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

The entity identified as the "Customer" in the DPA

(the "**data exporter**")

And

Everlaw, Inc.

2101 Webster Street, Suite 1500, Oakland, CA 94612, United States of America

e-mail: support@everlaw.com

(the "**data importer**")

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

1. 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];
2. 'the data exporter' means the controller who transfers the personal data;
3. 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
4. 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
5. 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
6. 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss,

alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

The data subject can enforce against the data exporter this Clause, Clause 4 to (i), Clause 5to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

The data subject can enforce against the data importer this Clause, Clause 5to and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

The data subject can enforce against the sub-processor this Clause, Clause 5to and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if

permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

1. that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
2. that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
3. that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
4. that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
5. that it will ensure compliance with the security measures;
6. that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
7. to forward any notification received from the data importer or any sub-processor pursuant to Clause 5and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

8. to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
9. that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
10. that it will ensure compliance with Clause 4to (i).

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

1. to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
2. that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
3. that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
4. that it will promptly notify the data exporter about:
    1. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

2. any accidental or unauthorised access, and
3. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

5. to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
6. at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
7. to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
8. that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
9. that the processing services by the sub-processor will be carried out in accordance with Clause 11;
10. to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognized sanctions, tax-reporting requirements

or anti-money-laundering reporting requirements.

Clause 6

Liability

The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a sub-processor of its obligation in order to avoid its own liabilities.

If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

1. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
2. to refer the dispute to the courts in the Member State in which the data exporter is established.

The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses[3]. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

[3] This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

Clause 12

Obligation after the termination of personal data processing services

The parties agree that on the termination of the provision of data processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data

and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and are agreed upon by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

For the purposes of this Appendix, "DPA" means the Data Processing Addendum in place between data importer and data exporter and to which these Clauses are incorporated.

Data exporter: The data exporter is the entity identified as the "Customer" in the DPA.

Data importer: Everlaw, Inc. is an e-discovery company based in the United States of America, who provides electronic discovery services to public and private entities for the purposes of supporting disclosure as provided under statute, regulation, or court order.

Data subjects: The data subjects are defined in Annex A of the DPA.

Categories of data: The personal data is defined in Annex A of the DPA.

Processing operations: The processing operations are defined in Annex A of the DPA.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4 and 5 (or document/legislation attached):

The technical and organisational security measures implemented by the

data importer are as described in the DPA.

APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix sets out the parties' interpretation of their respective obligations under specific Clauses identified below. Where a party complies with the interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the Clauses.

For the purposes of this Appendix, "DPA" means the Data Processing Addendum in place between data importer and data exporter and to which these Clauses are incorporated and "Agreement" shall have the meaning given to it in the DPA.

Clause 4(h) and 8: Disclosure of these Clauses

1. Data exporter agrees that these Clauses constitute data importer's Confidential Information as that term is defined in the Agreement and may not be disclosed by data exporter to any third party without data importer's prior written consent unless permitted pursuant to Agreement. This shall not prevent disclosure of these Clauses to a data subject pursuant to Clause 4(h) or a supervisory authority pursuant to Clause 8.

Clause 5: Suspension of data transfers and termination

1. The parties acknowledge that data importer may process the personal data only on behalf of the data exporter and in compliance with its instructions as provided by the data exporter and the Clauses.
2. The parties acknowledge that if data importer cannot provide such compliance for whatever reason, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract.
3. If the data exporter intends to suspend the transfer of personal data and/or terminate these Clauses, it shall endeavor to provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("Cure Period").
4. If after the Cure Period the data importer has not or cannot cure the non-compliance then the data exporter may suspend or terminate the transfer of personal data immediately. The data exporter shall not be required to provide such notice in instance where it considers there is a material risk of harm to data subjects or their personal

data.

Clause 5(f): Audit

1. Data exporter acknowledges and agrees that it exercises its audit right under Clause 5 by instructing data importer to comply with the audit measures described in Section 5 (Security Audits) of the DPA.

Clause 5(j): Disclosure of subprocessor agreements

1. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the Clauses to the data exporter.
2. The parties further acknowledge that, pursuant to subprocessor confidentiality restrictions, data importer may be restricted from disclosing onward subprocessor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any subprocessor it appoints to permit it to disclose the subprocessor agreement to data exporter.
3. Even where data importer cannot disclose a subprocessor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably in connection with such subprocessing agreement to data exporter.

Clause 6: Liability

1. Any claims brought under the Clauses shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement. In no event shall any party limit its liability with respect to any data subject rights under these Clauses.

Clause 11: Onward subprocessing

1. The parties acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 entitled "FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC" the data exporter may provide a general consent to onward subprocessing by the data importer.
2. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward subprocessors. Such consent is conditional on data importer's

compliance with the requirements set out in Section 3 (Sub-processing) of the DPA.

Subprocessor List

Infrastructure Subprocessors

Entity	Brief Description of Processing
Amazon Web Services, Inc.	Data hosting
Google Translate API	(Optional) Language translation feature which is offered as part of the Everlaw Service

Other Subprocessors

Entity	Brief Description of Processing
Zendesk	Customer service management and communications

Last updated: 4/28/2020

California Data Privacy Addendum

This California Data Privacy Addendum ("**CDPA**") forms part of the Customer Terms of Service available at https://www.everlaw.com/legal/terms, or a separate written agreement incorporating this CDPA by reference (the " **Agreement**"), by and between Everlaw, Inc., a Delaware corporation ("**Everlaw**") and the Customer named in the Agreement, pursuant to which Customer has purchased a subscription to access and use the Service (as defined in the Agreement).

Everlaw and Customer hereby agree to comply with the following provisions with respect to any information which qualifies as Personal Information of a Consumer (as defined below):

1. **Definitions.**
    1. "**CCPA**" means the California Consumer Privacy Act 2018 as set forth in California Civil Code § 1798.100 et seq. and all other applicable laws or regulations relating to the Processing of Personal Information that may exist in the relevant jurisdiction.
    2. "**Business**," "**Business Purpose**," "**Consumer**," "**Person**,"

"**Personal Information**" "**Sell**," "**Service Provider**" and "**Third Party**" shall have the meanings set forth in the CCPA.

3. All other defined terms shall have the meanings set forth in the Agreement.

2. **Terms.**
    1. The terms of this CDPA shall take effect upon January 1, 2020 and continue on concurrently for the term of the Agreement.
    2. The parties agree that Customer is a Business and Everlaw is its Service Provider in relation to this CDPA and Personal Information that is Processed in the course of Everlaw's provision of the Services set forth in the Agreement. The parties agree to comply at all times with the applicable provisions of the CCPA in respect to the collection, transmission, and processing of all Personal Information exchanged or shared pursuant to the Agreement.
    3. The subject-matter of the Processing of Personal Information covered by this CDPA is the Services ordered by Customer through Everlaw and provided by Everlaw to Customer as set out in the Agreement.
    4. Everlaw certifies that it understands the restrictions set forth in Section 1798.140(w)(2)(A) of the CCPA and will comply with them.
    5. Everlaw shall not Sell Personal Information.
    6. In respect of Personal Information Processed in the course of providing the Services, Everlaw:
        1. shall Process Personal Information only in accordance with the documented instructions from Customer (as set out in this CDPA or the Agreement or as otherwise notified by Customer to Everlaw from time to time); provided Everlaw may Process Personal Information for Business Purposes under the CCPA or another applicable law or regulation, and in such cases Everlaw will inform Customer of such requirement prior to the Processing unless that law prohibits this on important grounds of public interest;
        2. may hire other companies to provide limited services on its behalf, provided that Everlaw complies with the provisions of this clause. Any such subcontractors will be permitted to Process Personal Information only to deliver the Services. Everlaw remains responsible for its subcontractors' compliance with the obligations of this CDPA, and Everlaw shall ensure that any subcontractors to whom Everlaw transfers Personal Information will have

entered into written agreements with Everlaw requiring that the subcontractor abide by terms substantially similar to this CDPA; and

3. shall reasonably assist the Customer with its obligation to respond to requests from Consumers under the CCPA (including requests for information relating to the Processing, and requests relating to access, rectification, erasure or portability of the Personal Information) provided that Everlaw reserves the right to reimbursement from Customer for the reasonable cost of any time, expenditures or fees incurred in connection with such assistance.

3. **Miscellaneous**
    1. Except as expressly provided in this CDPA, the parties intend no amendment or modification of the Agreement or in such other addendum or supplement which may have been signed by the parties.
    2. Any notice to be provided under this CDPA to Customer shall be sent via email to the email address associated with Customer's account.
    3. This CDPA supplements the terms of the Agreement. In the event of any conflict between this CDPA and the Agreement regarding the processing of Consumers' Personal Information, the terms of this CDPA shall control.
    4. If any provision of this CDPA is held by a court of competent jurisdiction to be contrary to the law, the provision shall be modified by the court and interpreted so as best to accomplish the objectives of the original provision to the fullest extent permitted by law, and the remaining provisions of this CDPA shall remain in full force and effect.
    5. No waiver under this CDPA will be valid or binding unless set forth in writing and duly executed by the party against whom enforcement of such waiver is sought. Any such waiver will constitute a waiver only with respect to the specific matter described therein and will in no way impair the rights of the party granting such waiver in any other respect or at any other time. Any delay or forbearance by either party in exercising any right hereunder will not be deemed a waiver of that right.

Last Updated: 4/28/2020

Business Associate Agreement

This Business Associate Agreement ("Agreement") is entered into as of [] by and between Everlaw, Inc., a Delaware corporation ("Business Associate") and , a ("Covered Entity"), which is a covered entity under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The parties are entering into this Agreement to assist the Covered Entity in complying with HIPAA, and to set forth Business Associate's obligations under the Health Information Technology for Economic and Clinical Health Act of 2009 (the "HITECH Act"), and 45 CFR Parts 160 and 164, Subpart C (the "Security Rule"), Subpart D (the "Data Breach Notification Rule"), and Subpart E (the "Privacy Rule") (collectively, the "HIPAA Regulations"). Terms used in this Agreement have the meanings given them in the HIPAA Regulations. This Agreement applies to any Protected Health Information Business Associate receives from Covered Entity, or creates, receives or maintains on behalf of Covered Entity, under its agreements with Covered Entity (the "Principal Agreements").

AGREEMENT

1. Business Associate may use and disclose Covered Entity's Protected Health Information to provide Covered Entity with the goods and services contemplated by the Principal Agreements. Except as expressly provided below, this Agreement does not authorize Business Associate make any use or disclosure of Protected Health Information that Covered Entity would not be permitted to make.
2. Business Associate will:
    1. Not use or further disclose Covered Entity's Protected Health Information except as permitted by the Principal Agreements or this Agreement, or as required by law;
    2. Use appropriate safeguards, and comply, where applicable, with the HIPAA Security Rule with respect to electronic Protected Health Information, to prevent use or disclosure of Covered Entity's Protected Health Information other than as provided for by the Principal Agreements or this Agreement;
    3. Report to Covered Entity within 5 days of discovery any use or disclosure of Covered Entity's Protected Health Information not provided for by the Principal Agreements or this Agreement of which it becomes aware, including breaches of unsecured Protected Health Information as required by the Data Breach Notification Rule (45 CFR § 164.410), and any security incident of which Business Associate becomes aware.
    4. Mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of this

Agreement or the HIPAA Regulations;

5. Ensure that any of Business Associate's subcontractors that create, receive, maintain, or transmit Protected Health Information on behalf of the Business Associate agree in writing to the same restrictions and conditions that apply to Business Associate with respect to such information, including compliance with the HIPAA Security Rule with respect to electronic Protected Health Information;
6. Make any Protected Health Information in a designated record set available to Covered Entity to enable Covered Entity to meet its obligation to provide access to the information in accordance with 45 CFR § 164.524;
7. Make any Protected Health Information in a designated record set available for amendment and incorporate any amendments to Protected Health Information as directed by Covered Entity pursuant to 45 CFR § 164.526;
8. Make available to Covered Entity the information concerning disclosures that Business Associate makes of Covered Entity's Protected Health Information required to enable Covered Entity to provide an accounting of disclosures in accordance with 45 CFR § 164.528;
9. To the extent that Business Associate carries out Covered Entity's obligations under the Privacy Rule, comply with the requirements of the Privacy Rule that apply to Covered Entity in the performance of such obligations;
10. Make Business Associate's internal practices, books, and records relating to Business Associate's use and disclosure of Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, available to the Secretary of the United States Department of Health and Human Services for purposes of determining Covered Entity's compliance with the HIPAA Regulations, and to the Covered Entity for purposes of determining Business Associate's compliance with this Agreement;
11. Limit its requests for and uses and disclosures of Covered Entity's Protected Health Information to the minimum necessary, and comply with any minimum necessary policies and procedures that covered entity provides to Business Associate;
12. Upon termination of the Principal Agreements, return or destroy all Covered Entity's Protected Health Information that Business Associate still maintains in any form and retain no

copies of such information or, if return or destruction is not feasible, extend the protections of this Agreement to that information and limit further use and disclosure to those purposes that make the return or destruction of the information infeasible.

3. Business Associate may de-identify PHI pursuant to 45 C.F.R. §164.514 and use the de-identified information for any lawful purpose Business Associate's use and disclosure of such de-identified personal information will not be subject to the requirements set forth in this Agreement.
4. If Covered Entity determines that Business Associate has violated a material term of this Agreement, Covered Entity may immediately terminate the Principal Agreements. This Agreement shall remain in effect as long as Business Associate maintains or has access to Covered Entity's Protected Health Information, regardless of the termination of the Principal Agreements.
5. This Agreement is to be interpreted in accordance with HIPAA, the HITECH Act, and the regulations promulgated thereunder, as amended from time to time.