

STATE OF NEVADA
DEPARTMENT OF HEALTH AND HUMAN SERVICES

BUSINESS ASSOCIATE ADDENDUM

BETWEEN

The Division of Health Care Financing and Policy
Herein after referred to as the "Covered Entity"

and

(Enter Business Name)
Herein after referred to as the "Business Associate"

PURPOSE. In order to comply with the requirements of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, and the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, Public Law 111-5 this Addendum is hereby added and made part of the Contract between the Covered Entity and the Business Associate. This Addendum establishes the obligations of the Business Associate and the Covered Entity as well as the permitted uses and disclosures by the Business Associate of protected health information it may possess by reason of the Contract. The Covered Entity and the Business Associate shall protect the privacy and provide for the security of protected health information disclosed to the Business Associate pursuant to the Contract and in compliance with HIPAA, the HITECH Act, and regulation promulgated there under by the U.S. Department of Health and Human Services ("HIPAA Regulations") and other applicable laws.

WHEREAS, the Business Associate will provide certain services to the Covered Entity, and, pursuant to such arrangement, the Business Associate is considered a business associate of the Covered Entity as defined in HIPAA Regulations; and

WHEREAS, the Business Associate may have access to and/or create, receive, maintain or transmit certain protected health information from or on behalf of the Covered Entity, in fulfilling its responsibilities under such arrangement; and

WHEREAS, HIPAA Regulations require the Covered Entity to enter into a Contract containing specific requirements of the Business Associate prior to the disclosure of protected health information; and

THEREFORE, in consideration of the mutual obligations below and the exchange of information pursuant to this Addendum and to protect the interests of both Parties, the Parties agree to all provisions of this Addendum.

I. DEFINITIONS. The following terms in this Addendum shall have the same meaning as those terms in the HIPAA Regulations: Breach, Data Aggregation, Designated Record Set, Disclosure, Electronic Health Record, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, Secretary, Subcontractor, Unsecured Protected Health Information, and Use.

1. **Business Associate** shall mean the name of the organization or entity listed above and shall have the meaning given to the term under the Privacy and Security Rule and the HITECH Act. For full definition refer to 45 CFR 160.103.
2. **Contract** shall refer to this Addendum and that particular contract to which this Addendum is made a part.
3. **Covered Entity** shall mean the name of the Division listed above and shall have the meaning given to such term under the Privacy Rule and the Security Rule, including, but not limited to 45 CFR 160.103.
4. **Parties** shall mean the Business Associate and the Covered Entity.

II. OBLIGATIONS OF THE BUSINESS ASSOCIATE

1. **Access to Protected Health Information.** The Business Associate will provide, as directed by the Covered Entity or an individual, access to inspect or obtain a copy of protected health information about the individual that is maintained in a designated record set by the Business Associate or its agents or subcontractors, in order to meet the requirements of HIPAA Regulations. If the Business Associate maintains an electronic health record, the Business Associate, its agents or subcontractors shall provide such information in electronic format to enable the Covered Entity to fulfill its obligations under HIPAA Regulations.
2. **Access to Records.** The Business Associate shall make its internal practices, books and records relating to the use and disclosure of protected health information available to the Covered Entity and to the Secretary for purposes of determining Business Associate's compliance with HIPAA Regulations.
3. **Accounting of Disclosures.** Upon request, the Business Associate and its agents or subcontractors shall make available to the Covered Entity or the individual information required to provide an accounting of disclosures in accordance with HIPAA Regulations.
4. **Agents and Subcontractors.** The Business Associate must ensure all agents and 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 the Business Associate with respect to such information. The Business Associate must implement and maintain sanctions against agents and subcontractors that violate such restrictions and conditions and shall mitigate the effects of any such violation as outlined under HIPAA Regulations.
5. **Amendment of Protected Health Information.** The Business Associate will make available protected health information for amendment and incorporate any amendments in the designated record set maintained by the Business Associate or its agents or subcontractors, as directed by the Covered Entity or an individual, in order to meet the requirements of HIPAA Regulations.
6. **Audits, Investigations, and Enforcement.** If the data provided or created through the execution of the Contract becomes the subject of an audit, compliance review, or complaint investigation by the Office of Civil Rights or any other federal or state oversight agency, the Business Associate shall notify the Covered Entity immediately and provide the Covered Entity with a copy of any protected health information that the Business Associate provides to the Secretary or other federal or state oversight agency concurrently, to the extent that it is permitted to do so by law. The Business Associate and individuals associated with the Business Associate are solely responsible for all civil and criminal penalties assessed as a result of an audit, breach or violation of HIPAA Regulations.
7. **Breach or Other Improper Access, Use or Disclosure Reporting.** The Business Associate must report to the Covered Entity, in writing, any access, use or disclosure of protected health information not permitted by the Contract, Addendum or HIPAA Regulations by Business Associate or its agents or subcontractors. The Covered Entity must be notified immediately upon discovery or the first day such breach or suspected breach is known to the Business Associate or by exercising reasonable diligence would have been known by the Business Associate in accordance with HIPAA Regulations. In the event of a breach or suspected breach of protected health information, the report to the Covered Entity must be in writing and include the following: a brief description of the incident; the date of the incident; the date the incident was discovered by the Business Associate; a thorough description of the unsecured protected health information that was involved in the incident; the number of individuals whose protected health information was involved in the incident; and the steps the Business Associate or its agent or subcontractor is taking to investigate the incident and to protect against further incidents. The Covered Entity will determine if a breach of unsecured protected health information has occurred and will notify the Business Associate of the determination. If a breach of unsecured protected health information is determined, the Business Associate must take prompt corrective action to cure any such deficiencies and mitigate any significant harm that may have occurred to individual(s) whose information was disclosed inappropriately.
8. **Breach Notification Requirements.** If the Covered Entity determines a breach of unsecured protected health information by the Business Associate, or its agents or

subcontractors has occurred, the Business Associate will be responsible for notifying the individuals whose unsecured protected health information was breached in accordance with HIPAA Regulations. The Business Associate must provide evidence to the Covered Entity that appropriate notifications to individuals and/or media, when necessary, as specified in HIPAA Regulations has occurred. The Business Associate is responsible for all costs associated with notification to individuals, the media or others as well as costs associated with mitigating future breaches. The Business Associate must notify the Secretary of all breaches in accordance with HIPAA Regulations and must provide the Covered Entity with a copy of all notifications made to the Secretary.

9. **Data Ownership.** The Business Associate acknowledges that the Business Associate or its agents or subcontractors have no ownership rights with respect to the protected health information it creates, receives or maintains, or otherwise holds, transmits, uses or discloses.
10. **Litigation or Administrative Proceedings.** The Business Associate shall make itself, any subcontractors, employees, or agents assisting the Business Associate in the performance of its obligations under the Contract or Addendum, available to the Covered Entity, at no cost to the Covered Entity, to testify as witnesses, or otherwise, in the event litigation or administrative proceedings are commenced against the Covered Entity, its administrators or workforce members upon a claimed violation by Business Associate of HIPAA Regulations or other laws relating to security and privacy.
11. **Minimum Necessary.** The Business Associate and its agents and subcontractors shall request, use and disclose only the minimum amount of protected health information necessary to accomplish the purpose of the request, use or disclosure in accordance with HIPAA Regulations.
12. **Policies and Procedures.** The Business Associate must adopt written privacy and security policies and procedures and documentation standards to meet the requirements of HIPAA Regulations.
13. **Privacy and Security Officer(s).** The Business Associate must appoint Privacy and Security Officer(s) whose responsibilities shall include: monitoring the Privacy and Security compliance of the Business Associate; development and implementation of the Business Associate's HIPAA Privacy and Security policies and procedures; establishment of Privacy and Security training programs; and development and implementation of an incident risk assessment and response plan in the event the Business Associate sustains a breach or suspected breach of protected health information.
14. **Safeguards.** The Business Associate must implement safeguards as necessary to protect the confidentiality, integrity and availability of the protected health information the Business Associate creates, receives, maintains, or otherwise holds, transmits, uses or discloses on behalf of the Covered Entity. Safeguards must include administrative safeguards (e.g., risk analysis and designation of security official), physical safeguards (e.g., facility access controls and workstation security), and technical safeguards (e.g., access controls and audit controls) to the confidentiality, integrity and availability of the protected health information, in accordance with HIPAA Regulations. Technical safeguards must meet the standards set forth by the guidelines of the National Institute of Standards and Technology (NIST). The Business Associate agrees to only use or disclose protected health information as provided for by the Contract and Addendum and to mitigate, to the extent practicable, any harmful effect that is known to the Business Associate, of a use or disclosure, in violation of the requirements of this Addendum as outlined in HIPAA Regulations.
15. **Training.** The Business Associate must train all members of its workforce on the policies and procedures associated with safeguarding protected health information. This includes, at a minimum, training that covers the technical, physical and administrative safeguards needed to prevent inappropriate uses or disclosures of protected health information; training to prevent any intentional or unintentional use or disclosure that is a violation of HIPAA Regulations; and training that emphasizes the criminal and civil penalties related to HIPAA breaches or inappropriate uses or disclosures of protected health information. Workforce training of new employees must be completed within 30 days of the date of hire and all employees must be trained at least annually. The Business Associate must maintain written records for a period of six years. These records must document each employee that received training and the date the training was provided or received.

16. **Use and Disclosure of Protected Health Information.** The Business Associate must not use or further disclose protected health information other than as permitted or required by the Contract or as required by law. The Business Associate must not use or further disclose protected health information in a manner that would violate the requirements of HIPAA Regulations.

III. PERMITTED AND PROHIBITED USES AND DISCLOSURES BY THE BUSINESS ASSOCIATE

The Business Associate agrees to these general use and disclosure provisions:

1. **Permitted Uses and Disclosures:**

- a. Except as otherwise limited in this Addendum, the Business Associate may use or disclose protected health information to perform functions, activities, or services for, or on behalf of, the Covered Entity as specified in the Contract, provided that such use or disclosure would not violate HIPAA Regulations, if done by the Covered Entity.
- b. Except as otherwise limited in this Addendum, the Business Associate may use or disclose protected health information received by the Business Associate in its capacity as a Business Associate of the Covered Entity, as necessary, for the proper management and administration of the Business Associate, to carry out the legal responsibilities of the Business Associate, as required by law or for data aggregation purposes in accordance with HIPAA Regulations.
- c. Except as otherwise limited by this Addendum, if the Business Associate discloses protected health information to a third party, the Business Associate must obtain, prior to making such disclosure, reasonable written assurances from the third party that such protected health information will be held confidential pursuant to this Addendum and only disclosed as required by law or for the purposes for which it was disclosed to the third party. The written agreement from the third party must include requirements to immediately notify the Business Associate of any breaches of confidentiality of protected health information to the extent it has obtained knowledge of such breach.
- d. The Business Associate may use or disclose protected health information to report violations of law to appropriate federal and state authorities, consistent with HIPAA Regulations.

2. **Prohibited Uses and Disclosures:**

- a. Except as otherwise limited in this Addendum, the Business Associate shall not disclose protected health information to a health plan for payment or health care operations purposes if the patient has required this special restriction and has paid out of pocket in full for the health care item or service to which the protected health information relates in accordance with HIPAA Regulations.
- b. The Business Associate shall not directly or indirectly receive remuneration in exchange for any protected health information, unless the Covered Entity obtained a valid authorization, in accordance with HIPAA Regulations that includes a specification that protected health information can be exchanged for remuneration.

IV. OBLIGATIONS OF THE COVERED ENTITY

1. The Covered Entity will inform the Business Associate of any limitations in the Covered Entity's Notice of Privacy Practices in accordance with HIPAA Regulations, to the extent that such limitation may affect the Business Associate's use or disclosure of protected health information.
2. The Covered Entity will inform the Business Associate of any changes in, or revocation of, permission by an individual to use or disclose protected health information, to the extent that such changes may affect the Business Associate's use or disclosure of protected health information.
3. The Covered Entity will inform the Business Associate of any restriction to the use or disclosure of protected health information that the Covered Entity has agreed to in

accordance with HIPAA Regulations, to the extent that such restriction may affect the Business Associate's use or disclosure of protected health information.

4. Except in the event of lawful data aggregation or management and administrative activities, the Covered Entity shall not request the Business Associate to use or disclose protected health information in any manner that would not be permissible under HIPAA Regulations, if done by the Covered Entity.

V. TERM AND TERMINATION

1. **Effect of Termination:**

- a. Except as provided in paragraph (b) of this section, upon termination of this Addendum, for any reason, the Business Associate will return or destroy all protected health information received from the Covered Entity or created, maintained, or received by the Business Associate on behalf of the Covered Entity that the Business Associate still maintains in any form and the Business Associate will retain no copies of such information.
 - b. If the Business Associate determines that returning or destroying the protected health information is not feasible, the Business Associate will provide to the Covered Entity notification of the conditions that make return or destruction infeasible. Upon a mutual determination that return or destruction of protected health information is infeasible, the Business Associate shall extend the protections of this Addendum to such protected health information and limit further uses and disclosures of such protected health information to those purposes that make return or destruction infeasible, for so long as the Business Associate maintains such protected health information.
 - c. These termination provisions will apply to protected health information that is in the possession of subcontractors, agents or employees of the Business Associate.
2. **Term.** The Term of this Addendum shall commence as of the effective date of this Addendum herein and shall extend beyond the termination of the contract and shall terminate when all the protected health information provided by the Covered Entity to the Business Associate, or accessed, maintained, created, retained, modified, recorded, stored or otherwise held, transmitted, used or disclosed by the Business Associate on behalf of the Covered Entity, is destroyed or returned to the Covered Entity, or if it is not feasible to return or destroy the protected health information, protections are extended to such information, in accordance with the termination.
 3. **Termination for Breach of Contract.** The Business Associate agrees that the Covered Entity may immediately terminate the Contract if the Covered Entity determines that the Business Associate has violated a material part of this Addendum.

VI. MISCELLANEOUS

1. **Amendment.** The parties agree to take such action as is necessary to amend this Addendum from time to time for the Covered Entity to comply with all the requirements of HIPAA Regulations.
2. **Clarification.** This Addendum references the requirements of HIPAA Regulations, as well as amendments and/or provisions that are currently in place and any that may be forthcoming.
3. **Indemnification.** Each party will indemnify and hold harmless the other party to this Addendum from and against all claims, losses, liabilities, costs and other expenses incurred as a result of, or arising directly or indirectly out of or in conjunction with:
 - a. Any misrepresentation, breach of warranty or non-fulfillment of any undertaking on the part of the party under this Addendum; and
 - b. Any claims, demands, awards, judgments, actions, and proceedings made by any person or organization arising out of or in any way connected with the party's performance under this Addendum.
4. **Interpretation.** The provisions of this Addendum shall prevail over any provisions in the Contract that any conflict or appear inconsistent with any provision in this Addendum. This Addendum and the Contract shall be interpreted as broadly as necessary to

implement and comply with HIPAA Regulations. The parties agree that any ambiguity in this Addendum shall be resolved to permit the Covered Entity and the Business Associate to comply with HIPAA Regulations.

5. **Regulatory Reference.** A reference in this Addendum to HIPAA Regulations means the sections as in effect or as amended.
6. **Survival.** The respective rights and obligations of Business Associate under Effect of Termination of this Addendum shall survive the termination of this Addendum.

IN WITNESS WHEREOF, the Business Associate and the Covered Entity have agreed to the terms of the above written agreement as of the effective date set forth below.

COVERED ENTITY

Division of Health Care Financing and Policy

1100 E. William Street, Suite 101

Carson City, NV 89701

(775) 684-3676

(775) 687-3735

(Authorized Signature)

Suzanne Bierman

Administrator

(Date)

BUSINESS ASSOCIATE

(Business Name)

(Business Address)

(City, State and Zip Code)

(Business Phone Number)

(Business FAX Number)

(Authorized Signature)

(Print Name)

(Title)

(Date)