

**STATE OF VERMONT
AUDITOR OF ACCOUNTS**

It is hereby agreed by the State of Vermont, Auditor of Accounts (hereafter called the "State") and KPMG LLP (hereafter called the "Contractor") that the contract between them commencing April 1, 2013, as amended, is hereby amended by adding Attachment E, Business Associate Agreement to the Contract.

Except as modified by this Amendment No. 1, all other provisions of the original contract remain in full force and effect.

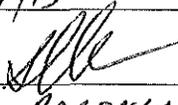
by the **STATE OF VERMONT:**

by the **CONTRACTOR:**

Date: 2/19/13

Date: 2/14/13

Signature: 
Douglas Hoffer
Auditor of Accounts

Signature: 
Name/Title: WARREN SHAW
Contractor: KPMG LLP WARREN



KPMG LLP
Two Financial Center
60 South Street
Boston, MA 02111

Telephone +1 617 988 1000
Fax +1 617 507 8321
Internet www.us.kpmg.com

January 4, 2013

Thomas M. Salmon, CPA
State Auditor
State of Vermont
132 State Street
Montpelier, Vermont 05633-5101

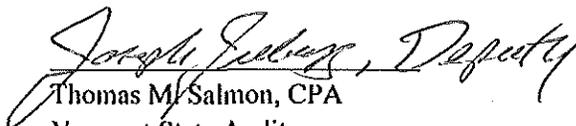
Dear Mr. Salmon:

Contract # 23700, entered into by the State Auditor, on behalf of the State of Vermont and by KPMG, is amended by adding Attachment E, Business Associate Agreement to the Contract.

Accepted by:



Shawn Warren, Partner
KPMG LLP



Thomas M. Salmon, CPA
Vermont State Auditor

1/4/13

Date

1/7/13

Date

ATTACHMENT E
BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") is entered into by and between the State of Vermont Auditor of Accounts ("Covered Entity") and KPMP LLP ("Business Associate") as of April 1, 2013 ("Effective Date"). This Agreement supplements and is made a part of the Contract to which it is an attachment.

Covered Entity and Business Associate enter into this Agreement to comply with standards promulgated under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") including the Standards for the Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164 ("Privacy Rule") and the Security Standards at 45 CFR Parts 160 and 164 ("Security Rule"), as amended by subtitle D of the Health Information Technology for Economic and Clinical Health Act.

The parties agree as follows:

1. **Definitions.** All capitalized terms in this Agreement have the meanings identified in this Agreement, 45 CFR Part 160, or 45 CFR Part 164.

The term "Services" includes all work performed by the Business Associate for or on behalf of Covered Entity that requires the use and/or disclosure of protected health information to perform a business associate function described in 45 CFR 160.103 under the definition of Business Associate.

The term "Individual" includes a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

The term "Breach" means the acquisition, access, use or disclosure of protected health information (PHI) in a manner not permitted under the HIPAA Privacy Rule, 45 CFR part 164, subpart E, which compromises the security or privacy of the PHI. "Compromises the security or privacy of the PHI" means poses a significant risk of financial, reputational or other harm to the individual.

2. **Permitted and Required Uses/Disclosures of PHI.**

- 2.1 Except as limited in this Agreement, Business Associate may use or disclose PHI to perform Services, as specified in the underlying contract with Covered Entity. Business Associate shall not use or disclose PHI in any manner that would constitute a violation of the Privacy Rule if used or disclosed by Covered Entity in that manner. Business Associate may not use or disclose PHI other than as permitted or required by this Agreement or as Required by Law.

- 2.2 Business Associate may make PHI available to its employees who need access to perform Services provided that Business Associate makes such employees aware of the use and disclosure restrictions in this Agreement and requires them to comply with such restrictions. Business Associate may only disclose PHI for the purposes authorized by this Agreement: (a) to its agents (including subcontractors) in accordance with Sections 8 and 16 or (b) as otherwise permitted by Section 3.

3. **Business Activities.** Business Associate may use PHI received in its capacity as a "Business Associate" to Covered Entity if necessary for Business Associate's proper management and administration or to carry out its legal responsibilities. Business Associate may disclose PHI received in its capacity as "Business Associate" to Covered Entity for Business Associate's proper management and administration or to carry out its legal responsibilities if a disclosure is Required by Law or if (a) Business Associate obtains reasonable written assurances via a written agreement from the person to whom the information is to be disclosed that the PHI shall remain confidential and be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person and (b) the person notifies Business Associate, within three business days (who in turn will notify Covered Entity within three business days after receiving notice of a Breach as specified in Section 5.1), in writing of any Breach of Unsecured PHI of which it is aware. Uses and disclosures of PHI for the purposes identified in this Section must be of the minimum amount of PHI necessary to accomplish such purposes.

4. **Safeguards.** Business Associate shall implement and use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for by this Agreement. With respect to any PHI that is maintained in or transmitted by

electronic media, Business Associate shall comply with 45 CFR sections 164.308 (administrative safeguards), 164.310 (physical safeguards), 164.312 (technical safeguards) and 164.316 (policies and procedures and documentation requirements). Business Associate shall summarize in writing upon request from Covered Entity the safeguards that it uses to prevent impermissible uses or disclosures of PHI. If additional information is needed by Covered Entity, Business Associate agrees that it shall allow an authorized representative of Covered Entity (approved by Business Associate) access to Business Associate's facilities to perform an onsite review of relevant policies and procedures. Business Associate will make every reasonable effort to be responsive to such inquiries, but reserves the right to limit disclosure of details and nature of procedures, if it determines, in its sole judgment, that such disclosure would place at risk the confidentiality of its own or its other clients' data.

5. Documenting and Reporting Breaches.

5.1 Business Associate shall report to Covered Entity any Breach of Unsecured PHI as soon as possible upon it (or any of its employees other than the individual committing the breach) becoming aware of any such Breach by KPMG or agent, and in no case later than three (3) business days after it (or any of its employees) becomes aware of the Breach, except when a law enforcement official determines that a notification would impede a criminal investigation or cause damage to national security.

5.2 To the extent known, Business Associate shall provide Covered Entity with the names of the individuals whose Unsecured PHI has been, or is reasonably believed to have been, the subject of the Breach and any other available information that is required to be given to the affected individuals, as set forth in 45 CFR §164.404(c), and, if requested by Covered Entity, information necessary for Covered Entity to investigate the impermissible use or disclosure. Business Associate shall continue to provide to Covered Entity information concerning the Breach as it becomes available to it.

5.3 When Business Associate determines that an impermissible acquisition, use or disclosure of PHI by a member of its workforce does not pose a significant risk of harm to the affected individuals, it shall document its assessment of risk. Such assessment shall include: 1) the name of the person(s) making the assessment, 2) a brief summary of the facts, and 3) a brief statement of the reasons supporting the determination of low risk of harm. When requested by Covered Entity, Business Associate shall make its risk assessments available to Covered Entity.

6. Mitigation and Corrective Action. Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to it of an impermissible use or disclosure of PHI, even if the impermissible use or disclosure does not constitute a Breach. Business Associate shall draft and carry out a reasonable plan of corrective action to address any incident of impermissible use or disclosure of PHI. If requested by Covered Entity, Business Associate shall make its mitigation and corrective action plans available to Covered Entity.

7. Providing Notice of Breaches.

7.1 If Covered Entity determines that an impermissible acquisition, access, use or disclosure of PHI for which one of Business Associate's employees or agents was responsible constitutes a Breach as defined in 45 CFR §164.402, and if requested by Covered Entity, Business Associate shall directly or through an authorized agent provide notice to the individuals whose PHI was the subject of the Breach. Such notice will be in accordance with Covered Entity's instructions and 45 CFR Part 164, Subpart D. When requested to provide notice, Business Associate shall consult with Covered Entity about the timeliness, content and method of notice, and shall receive Covered Entity's approval concerning these elements. The cost of notice and related remedies shall be borne by Business Associate.

7.2 The notice to affected individuals shall be provided as soon as reasonably possible and in no case later than 60 calendar days after Business Associate reported the Breach to Covered Entity.

7.3 The notice to affected individuals shall be written in plain language and shall include, to the extent possible, 1) a brief description of what happened, 2) a description of the types of Unsecured PHI that were involved in the Breach, 3) any steps individuals can take to protect themselves from potential harm resulting from the Breach, 4) a brief description of what the Business associate is doing to investigate the Breach, to mitigate harm to individuals and to protect against further Breaches, and 5) contact procedures for individuals to ask questions or obtain additional information, as set forth in 45 CFR §164.404(c).

7.4 Business Associate shall notify individuals of Breaches as specified in 45 CFR §164.404(d) (methods of

individual notice). In addition, when a Breach involves more than 500 residents of Vermont, Business associate shall, if requested by Covered Entity, notify prominent media outlets serving Vermont, following the requirements set forth in 45 CFR §164.406.

8. **Agreements by Third Parties.** Business Associate shall ensure that any agent (including a subcontractor) to whom it provides PHI received from Covered Entity or created or received by Business Associate on behalf of Covered Entity agrees in a written agreement to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such PHI. For example, the written contract must include those restrictions and conditions set forth in Section 14. Business Associate must enter into the written agreement before any use or disclosure of PHI by such agent. The written agreement must identify Covered Entity as a direct and intended third party beneficiary with the right to enforce any breach of the agreement concerning the use or disclosure of PHI. Business Associate shall provide a copy of the written agreement to Covered Entity upon request. Business Associate may not make any disclosure of PHI to any agent without the prior written consent of Covered Entity. This requirement regarding prior written consent does not apply to an agent with whom Business Associate has entered into a contract prior to the effective date of this contract, and under which the Business Associate will provide to the agent PHI that Business Associate received from Covered Entity or that it created or received on behalf of Covered Entity.
9. **Access to PHI.** Business Associate shall provide access to PHI in a Designated Record Set to Covered Entity to meet the requirements under 45 CFR 164.524. Business Associate shall provide such access in the time and manner reasonably designated by Covered Entity. Within three (3) business days, Business Associate shall forward to Covered Entity for handling any request for access to PHI that Business Associate directly receives from an Individual.
10. **Amendment of PHI.** Business Associate shall make any amendments to PHI in a Designated Record Set that Covered Entity directs or agrees to pursuant to 45 CFR 164.526, at the request of Covered Entity. Business Associate shall make such amendments in the time and manner reasonably designated by Covered Entity. Within three (3) business days, Business Associate shall forward to Covered Entity for handling any request for amendment to PHI that Business Associate directly receives from an Individual.
11. **Accounting of Disclosures.** Business Associate shall document disclosures of PHI and all information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR 164.528. Business Associate shall provide such information to Covered Entity to permit Covered Entity to respond to an accounting request. Business Associate shall provide such information in the time and manner reasonably designated by Covered Entity. Within three (3) business days, Business Associate shall forward to Covered Entity for handling any accounting request that Business Associate directly receives from an Individual.
12. **Books and Records.** Subject to the attorney-client and other applicable legal privileges, Business Associate shall make its internal practices, books, and records (including policies and procedures and PHI) relating to the use and disclosure of PHI received from Covered Entity or created or received by Business Associate on behalf of Covered Entity available to the Secretary in the time and manner designated by the Secretary. Business Associate shall make the same information available to Covered Entity upon Covered Entity's request in the time and manner reasonably designated by Covered Entity so that Covered Entity may determine whether Business Associate is in compliance with this Agreement.
13. **Termination.**
 - 13.1 This Agreement commences on the Effective Date and shall remain in effect until terminated by Covered Entity or until all of the PHI provided by Covered Entity to Business Associate or created or received by Business Associate on behalf of Covered Entity is destroyed or returned to Covered Entity subject to Section 17.7.
 - 13.2 If one party breaches any material term of this Agreement, the non-breaching party may either: (a) provide an opportunity for the breaching party to cure the breach and terminate this Agreement or the Contract without liability or penalty if the breaching party does not cure the breach within the time specified by the non-breaching party; or (b) immediately terminate this Contract without liability or penalty if cure is not reasonably possible; or (c) if neither termination nor cure are feasible, the non-breaching party report the breach to the Secretary. The non-breaching party has the right to seek to cure any breach by the breaching party and this right, regardless of whether the non-breaching party cures such breach, does not lessen any right or remedy

available to the non-breaching party at law, in equity, or under this Contract, nor does it lessen the breaching party's responsibility for such breach or its duty to cure or if cure is not possible, mitigate, such breach.

14. Return/Destruction of PHI.

14.1 Except as permitted by 14.2, Business Associate in connection with the expiration or termination of this Contract shall return or destroy, at the discretion of the Covered Entity, all PHI received from Covered Entity or created or received by Business Associate on behalf of Covered Entity pursuant to this Contract that Business Associate still maintains in any form or medium (including electronic) within thirty (30) days after such expiration or termination. Business Associate shall not retain any copies of the PHI. Business Associate shall certify in writing for Covered Entity (1) when all PHI has been returned or destroyed and (2) that Business Associate does not continue to maintain any PHI. Business Associate is to provide this certification during this thirty (30) day period.

14.2 Business Associate shall provide to Covered Entity notification of any conditions that Business Associate believes make the return or destruction of PHI infeasible. If Covered Entity agrees that return or destruction is infeasible, Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible for so long as Business Associate maintains such PHI. The parties agree that it is infeasible for Business Associate to return or destroy PHI in its work papers, and no further notification nor Covered Entity agreement is necessary regarding the retention of such PHI.

15. Penalties and Training. Business Associate understands that: (a) there may be civil or criminal penalties for misuse or misappropriation of PHI and (b) violations of this Agreement may result in notification by Covered Entity to law enforcement officials and regulatory, accreditation, and licensure organizations. If requested by Covered Entity, Business Associate shall participate in training regarding the use, confidentiality, and security of PHI.

16. Security Rule Obligations. The following provisions of this Section apply to the extent that Business Associate creates, receives, maintains or transmits Electronic PHI on behalf of Covered Entity.

16.1 Business Associate shall implement and use administrative, physical, and technical safeguards in compliance with 45 CFR sections 164.308, 164.310, and 164.312 with respect to the Electronic PHI that it creates, receives, maintains or transmits on behalf of Covered Entity. Business Associate shall summarize in writing upon request from Covered Entity the safeguards that it uses to protect such Electronic PHI. If additional information is needed by Covered Entity, Business Associate agrees that it shall allow an authorized representative of Covered Entity (approved by Business Associate) access to Business Associate's facilities to perform an onsite review of relevant policies and procedures. Business Associate will make every reasonable effort to be responsive to such inquiries, but reserves the right to limit disclosure of details and nature of procedures, if it determines, in its sole judgment, that such disclosure would place at risk the confidentiality of its own or its other clients' data.

16.2 Business Associate shall ensure that any agent (including a subcontractor) to whom it provides Electronic PHI agrees in a written agreement to implement and use administrative, physical, and technical safeguards that reasonably and appropriately protect the Confidentiality, Integrity and Availability of the Electronic PHI. Business Associate must enter into this written agreement before any use or disclosure of Electronic PHI by such agent. The written agreement must identify Covered Entity as a direct and intended third party beneficiary with the right to enforce any breach of the agreement concerning the use or disclosure of Electronic PHI. Business Associate shall provide a copy of the written agreement to Covered Entity upon request. Business Associate may not make any disclosure of Electronic PHI to any agent without the prior written consent of Covered Entity. This requirement regarding prior written consent does not apply to an agent with whom Business Associate has entered into a contract prior to the effective date of this contract, and under which the Business Associate will provide to the agent PHI that Business Associate received from Covered Entity or that it created or received on behalf of Covered Entity.

16.3 Business Associate shall report in writing to Covered Entity any Security Incident pertaining to such Electronic PHI (whether involving Business Associate or an agent, including a subcontractor). Business Associate shall provide this written report as soon as it becomes aware of any such Security Incident, and in no case later than three (3) business days after it becomes aware of the incident. Business Associate shall provide Covered Entity with the information necessary for Covered Entity to investigate any such Security Incident.

STATE OF VERMONT
CONTRACT FOR SERVICES

16.4 Business Associate shall comply with any reasonable policies and procedures Covered Entity implements to obtain compliance under the Security Rule that apply to access by Business Associate of Covered Entity's systems.

17. Miscellaneous.

17.1 In the event of any conflict or inconsistency between the terms of this Agreement and the terms of the Contract, the terms of this Agreement shall govern with respect to its subject matter. Otherwise the terms of the Contract continue in effect.

17.2 Business Associate shall cooperate with Covered Entity to amend this Agreement from time to time as is necessary for the parties to comply with applicable provisions of the Privacy Rule, the Security Rule, or any other standards promulgated under HIPAA and HITECH.

17.3 Any ambiguity in this Agreement shall be resolved to permit compliance with the Privacy Rule, Security Rule, or any other standards promulgated under HIPAA and HITECH.

17.4 In addition to applicable Vermont law, the parties shall rely on applicable federal law (e.g., HIPAA, the Privacy Rule and Security Rule) in construing the meaning and effect of this Agreement.

17.5 As between Business Associate and Covered Entity, Covered Entity owns all PHI provided by Covered Entity to Business Associate or created or received by Business Associate on behalf of Covered Entity.

17.6 Business Associate shall abide by the terms and conditions of this Agreement with respect to all PHI it receives from Covered Entity or creates or receives on behalf of Covered Entity under this Contract even if some of that information relates to specific services for which Business Associate may not be a "Business Associate" of Covered Entity under the Privacy Rule.

17.7 The provisions of this Agreement that by their terms encompass continuing rights or responsibilities shall survive the expiration or termination of this Agreement. For example: (a) the provisions of this Agreement shall continue to apply if Covered Entity determines that it would be infeasible for Business Associate to return or destroy PHI as provided in Section 14.2 and (b) the obligation of Business Associate to provide an accounting of disclosures as set forth in Section 11 survives the expiration or termination of this Agreement