

STATE OF VERMONT  
CONTRACT AMENDMENT

It is hereby agreed by and between the State of Vermont, Department of Vermont Health Access (the "State") and Capitol Health Associates, LLC with a principal place of business in Washington, DC (the "Contractor") that the contract between them originally dated as of January 1, 2018, Contract # 35403, as amended to date, (the "Contract") is hereby amended as follows:

- I. **Maximum Amount.** The maximum amount payable under the Contract, wherever such reference appears in the Contract, shall be changed from \$2,114,518.56 to \$2,373,518.56, representing an increase of \$259,000.00.
- II. **Attachment A Section: Contact Persons for this Contract** are hereby deleted and replaced as follows:

	<u>State Fiscal Manager</u>	<u>State Program Manager</u>	<u>For the Contractor</u>
Name:	Susan Whitney	Timothy Tremblay	Hans Kastensmith
Phone #:	802-585-5491	802- 241-0230	703-622-6896
E-mail:	susan.whitney@vermont.gov	timothy.tremblay@vermont.gov	hck@capitolhealthdc.com

- III. **Attachment B, Payment Provisions.** The payment provisions are amended as follows:  
Attachment B is hereby deleted in its entirety and replaced as set forth in the attachment to this Amendment.
- IV. **Attachment E, Business Associate Agreement.** Attachment E is amended as follows:  
Attachment E is hereby deleted in its entirety and replaced by the Attachment E May 21, 2019 attached to this Amendment.

**Taxes Due to the State.** Contractor certifies under the pains and penalties of perjury that, as of the date this contract amendment is signed, the Contractor is in good standing with respect to, or in full compliance with a plan to pay, any and all taxes due the State of Vermont.

**Child Support (Applicable to natural persons only; not applicable to corporations, partnerships or LLCs).** Contractor is under no obligation to pay child support or is in good standing with respect to or in full compliance with a plan to pay any and all child support payable under a support order as of the date of this amendment.

**Certification Regarding Suspension or Debarment.** Contractor certifies under the pains and penalties of perjury that, as of the date this contract amendment is signed, neither Contractor nor Contractor's principals (officers, directors, owners, or partners) are presently debarred, suspended, proposed for debarment, declared ineligible or excluded from participation in federal programs, or programs supported in whole or in part by federal funds.

Contractor further certifies under pains and penalties of perjury that, as of the date this contract amendment is signed, Contractor is not presently debarred, suspended, nor named on the State's debarment list at: <http://bgs.vermont.gov/purchasing-contracting/debarment>

**STATE OF VERMONT  
DEPARTMENT OF VERMONT HEALTH ACCESS  
CAPITOL HEALTH ASSOCIATES, LLC**

**CONTRACT #35403  
AMENDMENT 1  
PAGE 2 OF 18**

SOV Cybersecurity Standard 19-01. All products and service provided to or for the use of the State under this Contract shall be in compliance with State of Vermont Cybersecurity Standard 19-01 and the Cybersecurity Standard Update 19-01 dated February 19, 2019, which Contractor acknowledges has been provided to it, and is available on-line at the following URL: <https://digitalservices.vermont.gov/cybersecurity/cybersecurity-standards-and-directives>

This document consists of 18 pages. Except as modified by this Amendment Number 1 all provisions of the Contract remain in full force and effect.

The signatures of the undersigned indicate that each has read and agrees to be bound by this Amendment to the Contract.

**DEPARTMENT OF VERMONT HEALTH ACCESS**

**CAPITOL HEALTH ASSOCIATES, LLC**

E-SIGNED by Cory Gustafson  
on 2019-12-31 13:48:13 GMT December 31, 2019

CORY GUSTAFSON, COMMISSIONER      DATE  
280 State Drive, NOB 1 South  
Waterbury, VT 05671-1010  
Phone: 802-241-0239  
Email: [cory.gustafson@vermont.gov](mailto:cory.gustafson@vermont.gov)

E-SIGNED by Hans Kastensmith  
on 2019-12-31 13:24:11 GMT December 31, 2019

HANS KASTENSMITH, MANAGING PARTNER DATE  
P.O. Box 425  
Oakton, VA 22124  
Phone: 703-622-6896  
Email: [hck@capitolhealthdc.com](mailto:hck@capitolhealthdc.com)

**ATTACHMENT B  
PAYMENT PROVISIONS**

The maximum dollar amount payable under this contract is not intended as any form of a guaranteed amount. Contractor will be paid for products actually delivered or services actually performed as specified in Attachment A up to the total maximum allowable amount specified in this contract. State payment terms are Net 30 days from date of invoice, payments against this contract will comply with State's payment terms. The payment schedule for delivered products, or rates for services performed, and any additional reimbursements, are included in this attachment. The following provisions specifying payments are:

1. The total maximum amount payable under this contract shall not exceed \$2,373,518.56.
2. Contractor shall submit invoices with a current date of submission, invoice number, and contract number on or by the 15<sup>th</sup> of each month for the prior month's expenses. Contractor shall invoice State monthly for staff time, travel, and operating expenses for work associated with tasks specified in Attachment A and Appendix II and this Attachment B. Invoices shall include the line item amount or the actual expenses incurred for each task, total hours worked per hourly-paid task, names of employees (as applicable) and a brief description of services performed, depending on the payment provisions, and the total amount billed.
3. Monthly invoices shall be accompanied by a completed financial reporting form (Appendix I: Required Forms, and as updated and provided to the Contractor by the State throughout the term of the contract). All reports and invoices related to this contract should be submitted in electronic format to the State Fiscal Manager and the State Program Manager specified in Attachment A of this contract.
4. Contractor shall be reimbursed based on a combination of defined monthly, hourly, or project-based amounts for each task (budget line item), milestone payments, and actual expenses incurred, as further set forth in this Attachment B, dependent on acceptance by State of monthly progress reports and deliverables as completed. Payment for activities under each task will only be issued after all monthly progress reports are received and accepted by State.
5. All payments to Contractor shall be based upon State's acceptance of the deliverables outlined in Attachment A and Appendix II.
6. State reserves the right to withhold part or all of the contract funds if State does not receive timely documentation of the successful completion of contract deliverables outlined in Attachment A and Appendix II. Any deliverables deemed unacceptable by State will be rejected and subject to revision by Contractor based upon a mutually agreed remediation plan.
7. Contractor will not be reimbursed for other expenses, including travel, supplies, benefits, or insurance, with the exception of cyber liability insurance, technology professional liability insurance, and software expenses explicitly specified in the below Budget Table of this Attachment B as payable on the basis of "documented, actual costs". Upon providing proof of payment and certifications of insurance, Contractor may invoice State up to the amount(s) specified in the Budget Table of this Attachment B for actual costs incurred to secure these items

8. Notwithstanding anything to the contrary in this Attachment B, and subject to the limitations described in this paragraph, the Blueprint Executive Director shall be entitled to increase or reduce any Budget Maximum specified in the Budget Table of this Attachment B with respect to any service or item for which either an hourly rate is specified or for which documented cost-based reimbursement applies; provided however, that (i) such permitted Budget Maximum adjustments may only be made within a particular SFY (not from one SFY to another), (ii) Total State Fiscal Year Budget amounts (as specified in the Budget Table) may not be increased, (iii) aggregate permitted Budget Maximum adjustments shall not exceed \$20,000 in SFY 2018, \$40,000 in SFY 2019 and \$20,000 in SFY 2020, and (iv) the Blueprint Executive Director must provide to the State Fiscal Manager and the contact person for the Contractor (identified in Attachment A) written notice describing the adjustments at least 30 days prior to the month in which the adjustments are proposed to become effective. The Blueprint Executive Director (or designee) shall maintain an updated Budget Table reflecting any adjustments made under this paragraph, which updated Budget Table shall be deemed incorporated into this Attachment B immediately and without and further action.
9. State shall pay Contractor at the following rates:

**Task 1: Blueprint Data Quality Program Management**

**a:** Contractor may invoice State \$10,000 per month up to the amount(s) specified in the Budget Table of this Attachment B for Data Quality Program Management.

**b:** Contractor may invoice State, up to the amount(s) specified in the Budget Table of this Attachment B, for expert consultation from Dr. Craig Jones related to Data Quality, at a rate of \$200 per hour.

**c:** Contractor may invoice State, up to the amount(s) specified in the Budget Table of this Attachment B, for planning related to the transition of data quality management to Vermont Health Information Exchange (VHIE) collaborative services.

**Task 2: Project Management of Statewide Blueprint Data Quality Initiatives**

Contractor may invoice State \$4,000 per month up to the amount(s) specified in the Budget Table of this Attachment B for project management of statewide Blueprint data quality initiatives, including Sprints and data optimization projects.

**Task 3: Recruitment and Onboarding of New Blueprint Data Quality Initiatives**

Contractor may invoice State \$5,000 per month up to the amount(s) specified in the Budget Table of this Attachment B for recruitment and onboarding of new Blueprint data quality initiatives, including Sprints and data optimization projects.

**Task 4: Involvement in Projects Supporting Data Quality Work**

Contractor may invoice State \$6,000 per month up to the amount(s) specified in the Budget Table of this Attachment B for active engagement in projects supporting data quality work.

**Task 5: VCR Program, Project and Vendor Management**

**a:** Contractor may invoice State \$13,833.33 per month, up to the amount(s) specified in the Budget Table of this Attachment B, for VCR Program, Project, and Vendor Management activities. Those activities include, but are not limited to, State required project management (documentation deliverables for management of the VCR, including management of Contractor's subcontractors for this work.

**b:** Contractor may invoice State, up to the amount(s) specified in the Budget Table of this Attachment B, for expert consultation from Dr. Craig Jones related to Data Utilization, at a rate of \$200 per hour.

**Task 6: Hosting Management Services and General Operational Support for the VCR**

**a:** Contractor may invoice State \$2,475.00 per month, up to the amount(s) specified in the Budget Table of this Attachment B, for provision and management of hardware, software, and personnel resources required to maintain and operate the VCR, including hosting management and maintenance of fully functional versions of the VCR software in both a test and a production environment.

**b:** Contractor may invoice State for the documented, actual costs of license fees, upon proof of purchase and license, for the software required for successful operation of the VCR, up to the amount(s) specified in the Budget Table of this Attachment B. Such required software may include:

- SQL Server Enterprise (14 licenses).
- DocSite-specific third-party software, including:
  - Telerik
  - Active Reports Professional
  - MediSpan
  - Nevron Chart for .NET
  - EVO PDF
  - Others as required

**Task 7: Ongoing Security Assessments, Vulnerability Scans, and Remediation**

**a:** Contractor may invoice State up to a maximum of \$6,795.25 per quarterly scan for ongoing security assessments and vulnerability scans, up to the amount(s) specified in the Budget Table of this Attachment B.

**b:** The Contractor may invoice State, up to the amount(s) specified in the Budget Table of this Attachment B, for assessment support and remediation of findings from security assessments and vulnerability scans of the VCR, at a rate of \$150 per hour.

**Task 8: Ongoing Hosting of VCR**

Contractor may invoice State for hosting for the test and production environments of the VCR at a rate of \$11,669.94 per month, up to the amount(s) specified in the Budget Table of this Attachment.

**Task 9: Technical Support of VCR**

Contractor may invoice State up to the amount(s) specified in the Budget Table of this Attachment B for technical support of the VCR, including but not limited to maintenance and operations, enhancement requests, and database optimization, for the test and production environments, production and delivery of final data extracts, archiving of data and code, and delivery of the VCR source code and supporting documentation at a rate of \$150 per hour.

**Task 10: Vermont Clinical Registry User Support**

Contractor may invoice State \$3,300.00 per month, up to the amount(s) specified in the Budget Table of this Attachment B, for the maintenance of a Help Desk and provision of Tier 1-3 level user support for the VCR.

**Task 11: Delivery of Clinical Data Extracts from the VCR**

Contractor may invoice State up to the amount(s) specified in the Budget Table of this Attachment B for development and secure delivery of clinical data extracts, at a rate of \$150 per hour.

**Secure File Transfer Protocol (SFTP) Services**

Contractor may invoice State \$125 per month, up to the amount(s) specified in the Budget Table of this Attachment B, for the provision of Secure File Transfer Protocol ("SFTP") services in support of the VCR.

**Data Dictionary Analysis Tool**

Contractor may invoice State for the documented, actual costs of Data Dictionary Analysis Tool(s) for the VCR, up to the amount(s) specified in the Budget Table of this Attachment B.

**ICD-10 Clinical Mapping**

Contractor may invoice State for the documented, actual costs of ICD-10 Clinical Mapping for the VCR, up to the amount(s) specified in the Budget Table of this Attachment B.

**Practice Support for Flat File Extracts**

Contractor may invoice State up to the amount(s) specified in the Budget Table of this Attachment B for Practice support for flat file extracts for the VCR, at a rate of \$150 per hour.

**Cyber Liability and Related Professional Liability Insurance**

Upon providing proof of payment and certifications of insurance, Contractor may invoice State up to the amount(s) specified in the Budget Table of this Attachment B, for actual costs incurred to secure Cyber Liability and related Professional Liability Insurance in relation to the VCR.

10. Payments contingent on Blueprint-accepted data extracts. Expanded and full clinical data extracts from the VCR, which meet the specifications of Attachment A, Task 11, Deliverable 1 (Prime Deliverable), constitute the primary and ultimate deliverables for this contract. Payments for Tasks 5.a, 5.b, 6.a, 9, 10, and 11 of Attachment A of this contract will be contingent upon Contractor having delivered to State and/or its State-authorized designees a Prime Deliverable (accepted in writing by State) within 6 months prior to the invoice date, except in the case of invoices for the final month of the contract. In the case of invoices for the final month of the contract, payments for Tasks 5.a, 5.b, 6.a, 9, 10, and 11 will be contingent upon Contractor having delivered to State and/or its State-authorized designees a Prime Deliverable (accepted in

writing by State) in the final month of the contract or later. Contractor agrees that failure to deliver the products and services under this specific task (Task 11) will constitute a material breach of the contract.

11. Budget Maximums for certain line items below are subject to adjustment from time to time in the discretion of the Blueprint Executive Director pursuant to paragraph 8 of this Attachment B.

**Budget Table**

Task	Description	Unit Amount January 1, 2018 - June 30, 2018 (Second Half of SFY 2018)	Budget Maximum For Services Provided January 1, 2018 - June 30, 2018 (Second Half of SFY 2018)	Unit Amount July 1, 2018 - June 30, 2019 (SFY 2019)	Budget Maximum For Services Provided July 1, 2018 - June 30, 2019 (SFY 2019)	Unit Amount July 1, 2019 - December 31, 2019 (First Half of SFY 2020)	Budget Maximum For Services Provided July 1, 2019 - December 31, 2019 (First Half of SFY 2020)
	Number of Months	6		12		6	
1.a	Data Quality Program Management	\$10,000 per month	\$60,000.00	\$10,000 per month	\$120,000.00	\$10,000 per month	\$60,000.00
1.b	Dr. Jones Expert Consultation on Data Quality	\$200 per hour	\$12,000.00	\$200 per hour	\$24,000.00	\$200 per hour	\$12,000.00
1.c.	Planning for Transition of Data Quality Management to VHIE Collaborative Services					\$83,333.33 each, upon delivery of copies of fully executed (signed) VITL subcontracts for VHIE collaborative services components of i.) Universal Master Person Index, ii.) Terminology Services, and iii.) Rhapsody Integration Engine	\$250,000.00



Task	Description	Unit Amount January 1, 2018 - June 30, 2018 (Second Half of SFY 2018)	Budget Maximum For Services Provided January 1, 2018 - June 30, 2018 (Second Half of SFY 2018)	Unit Amount July 1, 2018 - June 30, 2019 (SFY 2019)	Budget Maximum For Services Provided July 1, 2018 - June 30, 2019 (SFY 2019)	Unit Amount July 1, 2019 - December 31, 2019 (First Half of SFY 2020)	Budget Maximum For Services Provided July 1, 2019 - December 31, 2019 (First Half of SFY 2020)
	Number of Months	6		12		6	
2	Project Management of Statewide Blueprint Data Quality Initiatives	\$4,000 per month	\$24,000.00	\$4,000 per month	\$48,000.00	\$4,000 per month	\$24,000.00
3	Recruitment and Onboarding of New Blueprint Data Quality Initiatives	\$5,000 per month	\$30,000.00	\$5,000 per month	\$60,000.00	\$5,000 per month	\$30,000.00
4	Involvement in Projects Supporting Data Quality Work	\$6,000 per month	\$36,000.00	\$6,000 per month	\$72,000.00	\$6,000 per month	\$36,000.00
5.a	VCR Program, Project, and Vendor Management	\$13,833.33 per month	\$83,000.00	\$13,833.33 per month	\$166,000.00	\$13,833.33 per month	\$83,000.00
5.b	Dr. Jones Expert Consultation on Data Utilization	\$200 per hour	\$12,000.00	\$200 per hour	\$24,000.00	\$200 per hour	\$12,000.00
6.a	Hosting Management Services and General Operational Support for the VCR	\$2,475.00 per month	\$14,850.00	\$2,475.00 per month	\$29,700.00	\$2,475.00 per month	\$14,850.00
6.b	Software licenses to operate VCR	documented, actual costs	\$1,990.00				

Task	Description	Unit Amount January 1, 2018 - June 30, 2018 (Second Half of SFY 2018)	Budget Maximum For Services Provided January 1, 2018 - June 30, 2018 (Second Half of SFY 2018)	Unit Amount July 1, 2018 - June 30, 2019 (SFY 2019)	Budget Maximum For Services Provided July 1, 2018 - June 30, 2019 (SFY 2019)	Unit Amount July 1, 2019 - December 31, 2019 (First Half of SFY 2020)	Budget Maximum For Services Provided July 1, 2019 - December 31, 2019 (First Half of SFY 2020)
	Number of Months	6		12		6	
7.a	Ongoing Security Assessments, Vulnerability Scans, and Remediation	\$6,795.25 per quarterly scan	\$13,590.50	\$6,931.25 per quarterly scan	\$27,725.00	\$7,067.25 per quarterly scan	\$14,134.50
7.b	Assessment Support and Remediation	\$150 per hour	\$13,200.00	\$150 per hour	\$26,400.00	\$150 per hour	\$13,200.00
8	Ongoing Hosting of VCR	\$11,669.94 per month	\$70,019.64	\$11,669.94 per month	\$140,039.28	\$11,669.94 per month	\$70,019.64
9	Technical Support of VCR, including Final Data Extracts, Archiving, and Delivery of VCR Source Code and Supporting Documentation	\$150 per hour	\$89,100.00	\$150 per hour	\$178,200.00	\$150 per hour	\$98,100.00
10	VCR User Support	monthly \$3,300.00 for support	\$19,800.00	monthly \$3,300.00 for support	\$39,600.00	monthly \$3,300.00 for support	\$19,800.00
11	Delivery of Clinical Data Extracts from the VCR	\$150 per hour	\$19,800.00	\$150 per hour	\$39,600.00	\$150 per hour	\$19,800.00
N/A	SFTP Services	\$125 per month	\$750.00	\$125 per month	\$1,500.00	\$125 per month	\$750.00

Task	Description	Unit Amount January 1, 2018 - June 30, 2018 (Second Half of SFY 2018)	Budget Maximum For Services Provided January 1, 2018 - June 30, 2018 (Second Half of SFY 2018)	Unit Amount July 1, 2018 - June 30, 2019 (SFY 2019)	Budget Maximum For Services Provided July 1, 2018 - June 30, 2019 (SFY 2019)	Unit Amount July 1, 2019 - December 31, 2019 (First Half of SFY 2020)	Budget Maximum For Services Provided July 1, 2019 - December 31, 2019 (First Half of SFY 2020)
	Number of Months	6		12		6	
N/A	Data Dictionary Analysis Tool	documented, actual costs	\$3,000.00				
N/A	ICD10 Clinical Mapping	documented, actual costs	\$6,000.00				
N/A	Practice Support for Flat File Extracts	\$150 per hour	\$7,500.00	\$150 per hour	\$15,000.00	\$150 per hour	\$7,500.00
N/A	Cyber Liability and Related Professional Liability Insurance	Documented, actual costs	\$20,000.00	Documented, actual costs	\$40,000.00	Documented, actual costs	\$20,000.00
Total State Fiscal Year Budget		\$536,600.14		\$1,051,764.28		\$785,154.14	
Total Contract Budget		\$2,373,518.56					

ATTACHMENT E  
BUSINESS ASSOCIATE AGREEMENT

SOV CONTRACTOR: Capitol Health Associates, LLC

SOV CONTRACT No. 35403      CONTRACT Effective DATE: January 1, 2018

THIS BUSINESS ASSOCIATE AGREEMENT ("AGREEMENT") IS ENTERED INTO BY AND BETWEEN THE STATE OF VERMONT AGENCY OF HUMAN SERVICES, OPERATING BY AND THROUGH ITS **DEPARTMENT OF VERMONT HEALTH ACCESS** ("COVERED ENTITY") AND PARTY IDENTIFIED IN THIS AGREEMENT AS CONTRACTOR ABOVE ("BUSINESS ASSOCIATE"). THIS AGREEMENT SUPPLEMENTS AND IS MADE A PART OF THE CONTRACT ("CONTRACT") TO WHICH IT IS ATTACHED.

Covered Entity and Business Associate enter into this Agreement to comply with the 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 (HITECH), and any associated federal rules and regulations.

**The parties agree as follows:**

**1. Definitions.** All capitalized terms used but not otherwise defined in this Agreement have the meanings set forth in 45 CFR Parts 160 and 164 as amended by HITECH and associated federal rules and regulations. Terms defined in this Agreement are italicized. Unless otherwise specified, when used in this Agreement, defined terms used in the singular shall be understood if appropriate in their context to include the plural when applicable.

"*Agent*" means an Individual acting within the scope of the agency of the *Business Associate*, in accordance with the Federal common law of agency, as referenced in 45 CFR § 160.402(c) and includes Workforce members and *Subcontractors*.

"*Breach*" means the acquisition, Access, Use or Disclosure of *Protected Health Information (PHI)* which compromises the Security or privacy of the *PHI*, except as excluded in the definition of *Breach* in 45 CFR § 164.402.

"*Business Associate*" shall have the meaning given for "Business Associate" in 45 CFR § 160.103 and means Contractor or Grantee and includes its Workforce, *Agents* and *Subcontractors*.

"*Electronic PHI*" shall mean *PHI* created, received, maintained or transmitted electronically in accordance with 45 CFR § 160.103.

"*Individual*" includes a Person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

"*Protected Health Information*" ("*PHI*") shall have the meaning given in 45 CFR § 160.103, limited to the *PHI* created or received by *Business Associate* from or on behalf of Covered Entity.

“*Required by Law*” means a mandate contained in law that compels an entity to make a use or disclosure of *PHI* and that is enforceable in a court of law and shall have the meaning given in 45 CFR § 164.103.

“*Report*” means submissions required by this Agreement as provided in section 2.3.

“*Security Incident*” means the attempted or successful unauthorized Access, Use, Disclosure, modification, or destruction of Information or interference with system operations in an Information System relating to *PHI* in accordance with 45 CFR § 164.304.

“*Services*” includes all work performed by the *Business Associate* for or on behalf of Covered Entity that requires the Use and/or Disclosure of *PHI* to perform a *Business Associate* function described in 45 CFR § 160.103.

“*Subcontractor*” means a Person to whom *Business Associate* delegates a function, activity, or service, other than in the capacity of a member of the workforce of such *Business Associate*.

“*Successful Security Incident*” shall mean a *Security Incident* that results in the unauthorized Access, Use, Disclosure, modification, or destruction of information or interference with system operations in an Information System.

“*Unsuccessful Security Incident*” shall mean a *Security Incident* such as routine occurrences that do not result in unauthorized Access, Use, Disclosure, modification, or destruction of information or interference with system operations in an Information System, such as: (i) unsuccessful attempts to penetrate computer networks or services maintained by *Business Associate*; and (ii) immaterial incidents such as pings and other broadcast attacks on *Business Associate's* firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above with respect to *Business Associate's* Information System.

“*Targeted Unsuccessful Security Incident*” means an *Unsuccessful Security Incident* that appears to be an attempt to obtain unauthorized Access, Use, Disclosure, modification or destruction of the Covered Entity's *Electronic PHI*.

**2. Contact Information for Privacy and Security Officers and Reports.**

2.1 *Business Associate* shall provide, within ten (10) days of the execution of this Agreement, written notice to the Contract or Grant manager the names and contact information of both the HIPAA Privacy Officer and HIPAA Security Officer of the *Business Associate*. This information must be updated by *Business Associate* any time these contacts change.

2.2 Covered Entity's HIPAA Privacy Officer and HIPAA Security Officer contact information is posted at: <http://humanservices.vermont.gov/policy-legislation/hipaa/hipaa-info-beneficiaries/ahs-hipaa-contacts/>

2.3 *Business Associate* shall submit all *Reports* required by this Agreement to the following email address: [AHS.PrivacyAndSecurity@vermont.gov](mailto:AHS.PrivacyAndSecurity@vermont.gov)

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

3.1 Subject to the terms in this Agreement, *Business Associate* may Use or Disclose *PHI* to perform *Services*, as specified in the Contract or Grant. Such Uses and Disclosures are limited to the minimum necessary to provide the *Services*. *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* and only in compliance with applicable laws and regulations.

3.2 *Business Associate* may make *PHI* available to its Workforce, *Agent* and *Subcontractor* who need Access to perform *Services* as permitted by this Agreement, provided that *Business Associate* makes them aware of the Use and Disclosure restrictions in this Agreement and binds them to comply with such restrictions.

3.3 *Business Associate* shall be directly liable under HIPAA for impermissible Uses and Disclosures of *PHI*.

4. **Business Activities.** *Business Associate* may Use *PHI* if necessary for *Business Associate's* proper management and administration or to carry out its legal responsibilities. *Business Associate* may Disclose *PHI* for *Business Associate's* proper management and administration or to carry out its legal responsibilities if a Disclosure is *Required by Law* or if *Business Associate* obtains reasonable written assurances via a written agreement from the Person to whom the information is to be Disclosed that such *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 the Agreement requires the Person to notify *Business Associate*, within five (5) business days, in writing of any *Breach* of Unsecured *PHI* of which it is aware. Such Uses and Disclosures of *PHI* must be of the minimum amount necessary to accomplish such purposes.

5. **Electronic PHI Security Rule Obligations.**

5.1 With respect to *Electronic PHI*, *Business Associate* shall:

- a) Implement and use Administrative, Physical, and Technical Safeguards in compliance with 45 CFR sections 164.308, 164.310, and 164.312;
- b) Identify in writing upon request from Covered Entity all the safeguards that it uses to protect such Electronic PHI;
- c) Prior to any Use or Disclosure of *Electronic PHI* by an *Agent* or *Subcontractor*, ensure that any *Agent* or *Subcontractor* to whom it provides *Electronic PHI* agrees in writing to implement and use Administrative, Physical, and Technical Safeguards that reasonably and appropriately protect the Confidentiality, Integrity and Availability of Electronic PHI. 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*, and be provided to Covered Entity upon request;
- d) Report in writing to Covered Entity any *Successful Security Incident* or *Targeted Security Incident* as soon as it becomes aware of such incident and in no event later than five (5) business days after such awareness. Such report shall be timely made notwithstanding the fact that little information may be known at the time of the report and need only include such information then available;
- e) Following such report, provide Covered Entity with the information necessary for Covered Entity to investigate any such incident; and
- f) Continue to provide to Covered Entity information concerning the incident as it becomes available to it.

5.2 Reporting *Unsuccessful Security Incidents*. *Business Associate* shall provide Covered Entity upon written request a *Report* that: (a) identifies the categories of Unsuccessful Security Incidents; (b) indicates whether *Business Associate* believes its current defensive security measures are adequate to address all Unsuccessful Security Incidents, given the scope and nature of such attempts; and (c) if the security measures are not adequate, the measures *Business Associate* will implement to address the security inadequacies.

5.3 *Business Associate* shall comply with any reasonable policies and procedures Covered Entity implements to obtain compliance under the Security Rule.

6. **Reporting and Documenting Breaches.**

6.1 *Business Associate* shall *Report* to Covered Entity any *Breach* of Unsecured *PHI* as soon as it, or any Person to whom *PHI* is disclosed under this Agreement, becomes aware of any such *Breach*, and in no event later than five (5) business days after such awareness, except when a law enforcement official determines that a notification would impede a criminal investigation or cause damage to national security. Such *Report* shall be timely made notwithstanding the fact that little information may be known at the time of the *Report* and need only include such information then available.

6.2 Following the *Report* described in 6.1, *Business Associate* shall conduct a risk assessment and provide it to Covered Entity with a summary of the event. *Business Associate* shall provide Covered Entity with the names of any *Individual* 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 *Individual*, as set forth in 45 CFR § 164.404(c). Upon request by Covered Entity, *Business Associate* shall provide 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.

6.3 When *Business Associate* determines that an impermissible acquisition, Access, Use or Disclosure of *PHI* for which it is responsible is not a *Breach*, and therefore does not necessitate notice to the impacted *Individual*, it shall document its assessment of risk, conducted as set forth in 45 CFR § 402(2). *Business Associate* shall make its risk assessment available to Covered Entity upon request. It shall include 1) the name of the person making the assessment, 2) a brief summary of the facts, and 3) a brief statement of the reasons supporting the determination of low probability that the *PHI* had been compromised.

7. **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 plan of corrective action to address any incident of impermissible Use or Disclosure of *PHI*. *Business Associate* shall make its mitigation and corrective action plans available to Covered Entity upon request.

8. **Providing Notice of Breaches.**

8.1 If Covered Entity determines that a *Breach* of *PHI* for which *Business Associate* was responsible, and if requested by Covered Entity, *Business Associate* shall provide notice to the *Individual* whose *PHI* has been the subject of the *Breach*. When so

requested, *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. *Business Associate* shall be responsible for the cost of notice and related remedies.

8.2 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.

8.3 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).

8.4 *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.

9. **Agreements with Subcontractors.** *Business Associate* shall enter into a Business Associate Agreement with any *Subcontractor* to whom it provides *PHI* to require compliance with HIPAA and to ensure *Business Associate* and *Subcontractor* comply with the terms and conditions of this Agreement. *Business Associate* must enter into such written agreement before any Use by or Disclosure of *PHI* to such *Subcontractor*. 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 it enters into with a *Subcontractor* to Covered Entity upon request. *Business Associate* may not make any Disclosure of *PHI* to any *Subcontractor* without prior written consent of Covered Entity.

10. **Access to PHI.** *Business Associate* shall provide access to *PHI* in a Designated Record Set to Covered Entity or as directed by Covered Entity to an *Individual* 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 five (5) 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*.

11. **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, whether at the request of Covered Entity or an *Individual*. *Business Associate* shall make such amendments in the time and manner reasonably designated by Covered Entity. Within five (5) 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*.



12. **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 or as directed by Covered Entity to an *Individual*, 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 five (5) business days, *Business Associate* shall forward to Covered Entity for handling any accounting request that *Business Associate* directly receives from an *Individual*.

13. **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* available to the Secretary of Health and Human Services (HHS) 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.

14. **Termination.**

14.1 This Agreement commences on the Effective Date and shall remain in effect until terminated by Covered Entity or until all the *PHI* is destroyed or returned to Covered Entity subject to Section 18.8.

14.2 If *Business Associate* fails to comply with any material term of this Agreement, Covered Entity may provide an opportunity for *Business Associate* to cure. If *Business Associate* does not cure within the time specified by Covered Entity or if Covered Entity believes that cure is not reasonably possible, Covered Entity may immediately terminate the Contract or Grant without incurring liability or penalty for such termination. If neither termination nor cure are feasible, Covered Entity shall report the breach to the Secretary of HHS. Covered Entity has the right to seek to cure such failure by *Business Associate*. Regardless of whether Covered Entity cures, it retains any right or remedy available at law, in equity, or under the Contract or Grant and *Business Associate* retains its responsibility for such failure.

15. **Return/Destruction of PHI.**

15.1 *Business Associate* in connection with the expiration or termination of the Contract or Grant shall return or destroy, at the discretion of the Covered Entity, *PHI* 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 *PHI*. *Business Associate* shall certify in writing and report to 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.

15.2 *Business Associate* shall report to Covered Entity any conditions that *Business Associate* believes make the return or destruction of *PHI* infeasible. *Business Associate* shall extend the protections of this Agreement to such *PHI* and limit further Uses and Disclosures to those purposes that make the return or destruction infeasible for so long as *Business Associate* maintains such *PHI*.

16. **Penalties.** *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.

17. **Training.** *Business Associate* understands its obligation to comply with the law and shall provide appropriate training and education to ensure compliance with this Agreement. If requested by Covered Entity, *Business Associate* shall participate in Covered Entity's training regarding the Use, Confidentiality, and Security of *PHI*; however, participation in such training shall not supplant nor relieve *Business Associate* of its obligations under this Agreement to independently assure compliance with the law and this Agreement.

18. **Miscellaneous.**

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

18.2 Each party shall cooperate with the other party to amend this Agreement from time to time as is necessary for such party to comply with the Privacy Rule, the Security Rule, or any other standards promulgated under HIPAA. This Agreement may not be amended, except by a writing signed by all parties hereto.

18.3 Any ambiguity in this Agreement shall be resolved to permit the parties to comply with the Privacy Rule, Security Rule, or any other standards promulgated under HIPAA.

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

18.5 *Business Associate* shall not have or claim any ownership of *PHI*.

18.6 *Business Associate* shall abide by the terms and conditions of this Agreement with respect to all *PHI* 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.

18.7 *Business Associate* is prohibited from directly or indirectly receiving any remuneration in exchange for an *Individual's PHI*. *Business Associate* will refrain from marketing activities that would violate HIPAA, including specifically Section 13406 of the HITECH Act. Reports or data containing *PHI* may not be sold without Covered Entity's or the affected Individual's written consent.

18.8 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 12 survives the expiration or termination of this Agreement with respect to accounting requests, if any, made after such expiration or termination.