l. **Parties.** This is a contract for personal services between the State of Vermont, Department of Vermont Health Access (hereafter called "State"), and Stone Environmental, Inc. with a principal place of business in Montpelier, VT (hereafter called "Contractor"). The Contractor's form of business organization is a corporation. The Contractor's local address is 535 Stone Cutters Way, Montpelier, Vermont 05602. It is the Contractor's responsibility to contact the Vermont Department of Taxes to determine if, by law, the Contractor is required to have a Vermont Department of Taxes Business Account Number.

2. **Subject Matter.** The subject matter of this contract is personal services generally on the subject of reproducing a production mode version of the already developed prototype for a web accessible database application and expanding that functionality to allow practices, project managers, and State staff to easily enter, track, and report on Blueprint practice, provider, and community health team data. Detailed services to be provided by the Contractor are described in Attachment A.

3. **Maximum Amount.** In consideration of the services to be performed by the Contractor, the State agrees to pay the Contractor, in accordance with the payment provisions specified in Attachment B, a sum not to exceed $161,150.

4. **Contract Term.** The period of the Contractor's performance shall begin on July 1, 2013 and end on June 30, 2015. Both the State and the Contractor have the option of extending this contract for one additional two-year term.

5. **Prior Approvals.** If approval by the Attorney General's Office, the Secretary of Administration, or the Department of Information and Innovation's Chief Information Officer is required, (under current law, bulletins, and interpretations), neither this contract nor any amendment to it is binding until it has been approved by such persons.

Approval by the Attorney General's Office is required.

Approval by the Secretary of Administration is required.

Approval by the Chief Officer of Information is required.

6. **Amendment.** No changes, modifications, or amendments in the terms and conditions of this contract shall be effective unless reduced to writing, numbered, and signed by the duly authorized representative of the State and Contractor.

7. **Cancellation.** This contract may be cancelled by either party by giving written notice at least 30 days in advance. Notwithstanding this provision, if a governmental agency with due authority determines that a program or facility operated by the Contractor, wherein services authorized under this contract are provided, is not in compliance with State and Federal law or is operating with deficiencies the State may terminate this contract immediately and notify the Contractor accordingly. Also, in the event that federal funds supporting this contract become unavailable or are reduced, the State may cancel this contract with no obligation to pay the Contractor from State revenues.

8. **Attachments.** This contract consists of 36 pages including the following attachments, which are incorporated herein:

Attachment A - Specifications of Work to be Performed

Attachment B - Payment Provisions
Attachment C - Customary State Contract provisions
Attachment E - Business Associate Agreement
Attachment F - Customary Contract Provisions of the Agency of Human Services
Attachment G - Original Contract #22886 Specifications of Work for Prototype

The order of precedence of documents shall be as follows:

1). This document
3). Attachment C
4). Attachment A
5). Attachment B
6). Attachment E
7). Attachment F
8). Attachment G

WE THE UNDERSIGNED PARTIES AGREE TO BE BOUND BY THIS CONTRACT.

BY THE STATE OF VERMONT:

E-SIGNED by Mark Larson
on 2013-07-09 13:51:20 GMT

MARK LARSON, COMMISSIONER DATE

BY THE CONTRACTOR:

E-SIGNED by David Healy
on 2013-07-09 13:18:48 GMT

DAVID HEALY, VICE PRESIDENT DATE

ATTACHMENT A

SPECIFICATIONS OF WORK TO BE PERFORMED

General Conditions

The Contractor will develop a web accessible database application that will allow practices, project managers, and State staff to easily enter, track, and report on Blueprint practice, provider, and community health team data.

The Contractor will provide the State with a User Administration package within the application. The State will then provide all users with a secure username and password, and each user will be assigned to a role that allows for a specific level of activity.

The application shall enforce a limit of (configurable) consecutive invalid access attempts by a user. The application shall protect against further, possibly malicious, user authentication attempts using an appropriate mechanism (e.g. locks the account/node until released by an administrator, locks the account/node for a configurable time period, or delays the next login prompt according to a configurable delay algorithm). The application shall also require users to change their passwords periodically as defined by State policy.

A directory of users and their assigned roles will be accessible within the application. Upon logging into the application, there will be various options for entering data. The application will contain multiple forms based on sheets currently contained in the “Readiness Database” Excel workbook maintained by the State.

Assumptions:

1. Before invoicing and payment commences, the Contractor will provide Craig Benson, Agency of Human Services (AHS) Data Services Director, with a completed/updated Data Dictionary via email to Craig.Benson@state.vt.us, subject to State review and approval. A preliminary Data Dictionary has been created and associated with this contract, but is subject to validation by both the Contractor and the State and is expected to undergo updates during the application design and development process (Task 1 below).
2. All work products (deliverables) are subject to review and approval by the State before being accepted. Each work product will be evaluated based on any and all descriptions listed within Attachment A, as well as all direction and input discussed and agreed upon between the State and the Contractor during the term of this Agreement as it aligns with the specifications of work. Any work product deemed unacceptable by the State will be subject to revision by the Contractor based upon a remediation plan that the State and the Contractor will develop. Payment will be contingent upon the State accepting each work product and any stipulations within Attachment B of this Agreement.
3. The State will work with Contractor to make decisions quickly so that efficient use of project resources is possible.

4. State will assign a Project Manager who will serve as the single point of contact for Contractor and who will be responsible for organizing the State resources necessary for the project including scheduling project meetings, requirements workshops, sign-off on requirements, User Acceptance Testing (UAT), etc.
5. The outcome of any of the Design Steps may reveal budget shortfalls for completing all applications.

Project tasks (linked to "Contract Deliverables" in Attachment B) are as follows:

Task 1: Complete Database and Blueprint Web Application Design and Development

The Contractor will work with the State Blueprint staff to expand the database and functionality of the Prototype Blueprint Database Application. (Attachment G contains the original specifications and scope of work for the prototype delivered to the Blueprint.) This task will include identifying which additional components of the Blueprint readiness database should be incorporated into the application (contact management). For each data component, the following items need to be determined:

- The State will provide a description for each data field and either valid versus invalid field values or a designation of a free-text field (no data validation required). The Contractor will then provide data validation for each data field (when specified as necessary by the State) to notify the user via a warning symbol and a message in red text specifying the exact formatting requirements for data entry when the user attempts to exit a field;
- Appropriate labels and ordering of fields for forms;
- Lookup values when appropriate, including dictionary constants and drop-down menus;
- Specific language for data field tool tips to anticipate/address user needs;
- Identification of which user roles have access to the data.

Deliverable: Complete Blueprint application design

Task 2: Complete Database and Front End Forms

Based on the design and specifications created in Task 1, the Contractor will create a front end user interface and back end database. This task will include the following:

- Data import from the State's "Readiness Database";
- A complete review of the application with respect to the State's security requirements and any required modifications to the existing code;
- Ensure the Blueprint for Health logo appears on every form;
- Design a streamlined and intuitive (self-explanatory) user interface that provides a simplified workflow for the end user;
- Address validation with the State's E911 addressing system to ensure that all physical addresses are valid and that the data is in the application.

***Deliverable*:** Complete database and front-end forms

Task 3: Develop Reporting System for Blueprint Database Application

The Blueprint office is required to submit reports to Medicare regarding all changes to Blueprint practices and providers. The Contractor will develop a system for tracking all database changes, including edits to existing records and new records added. Changes to every field in the database will be audited. The State needs to be able to retrieve a report of any changes made to the database, including, but not limited to:

- Any changes to any field from a correction in a National Provider Identifier (NPI)
- A change in the spelling of a practice name
- A new provider being added to a practice

The Change Audit report will need to be run for a specific date range and must include the following information:

- Record Type (Practice, Provider, CHT, etc.)
- Record Name (Practice Name, Provider Name, CHT Name, etc.)
- Field Label
- Date Changed
- Time Changed
- User Who Made Change
- Old Field Value
- New Field Value

On request, the Contractor will provide access to all data in the database to the State in a workable format, such as a .csv file for Excel. The Contractor will also provide guidance to the State on the efficient use of other tools that the State can use to write custom queries on this data.

The Contractor will work with Blueprint staff to identify additional data reporting requirements and formatting for reports up to the budgeted amount for this deliverable.

Deliverable: Complete reporting system

Task 4: User Testing, Acceptance, Application Refinement, and Deployment

Upon completion of the application, the State will test all aspects of the application to ensure that it meets the requirements outlined in the scope of work and design as specified in Tasks 1, 2, and 3. A single point of contact at the State, preferably the State PM (Data Management/Analyst), will report application defects to the Contractor PM (Database Application Developer). The Contractor will respond to bug fixes within this scope of effort according to defect priority as defined in the following table:

Priority	Definition	Fix Turnaround Time (from defect reporting date)
Critical	Results in a complete application outage and/or is detrimental to the majority of the development and/or testing efforts. There is no workaround.	3 business days during development, 1 business day once in production
Serious	Application functionality is degraded with severe adverse impact to the user and there is not an effective workaround.	7 business days during development, 3 business days once in production
Moderate	Application functionality is degraded with a moderate adverse impact to the user but there is an effective workaround.	15 business days during development, 10 business days once in production
Minor	No immediate adverse impact to the user.	20 business days
Request	Enhancement or change request	As agreed upon based on application maintenance budget

The State may provide the Contractor with a list of changes that would further refine needs beyond this work scope and request a cost estimate for those enhancements. All changes will be attached to this contract in the form of an amendment signed by both parties prior to the start of any work.

The Contractor will not be allowed to take the application into production until they have proven their systems and implementations are stable in a development and/or test environment.

The application will be installed on Contractor's servers in a production environment. The application shall be scalable and adaptable to meet future growth and expansion/contraction needs such that the application can be expanded on demand and be able to retain its performance levels when adding additional users, functions, and data. The application shall be designed to support the planned Vermont systems and any anticipated expansion in scope of connectivity.

Deliverable: Installed application on production server and acceptance by the State

Task 5: Documentation and Training

This task includes documentation as required by the State, including user manuals, a finalized data dictionary, and documentation of the application and database architecture.

Additionally, the application's error messages shall be expressed in plain language, precisely indicate the problem, and constructively suggest a solution.

The Contractor will provide training to State staff and other users in the use of the database application. Two 2-hour training sessions have been budgeted.

Deliverable: Training to State staff and complete documentation, including finalized data dictionary

Task 6: Project Management

The Contractor will provide a full annual project plan with major milestones defined for tracking against scope and schedule no later than July 30, 2013. This project plan is subject to approval by the State and will require input from State resources assigned to the project.

The Contractor will provide biweekly status reports substantiating the status and progress of the work until final completion of deliverables. A telephone call from the Contractor to the State will follow to review the progress report, which will then be followed up with the written resolution of any issues identified. The Contractor will inform the State Project Manager in writing of any substantive issues when encountered within three (3) business days. The progress report will be written in Microsoft Word, and a link to the file, along with any additional attachments, such as a Gantt chart, shall be emailed to the State PM and shall contain the following information:

- E-mail subject line: SOW Requesting Agency name, IT service category name; reporting period, and “Progress Report”;
- Work accomplished during the frequency period;
- Deliverable progress as a percentage of completion;
- Problem areas, including scope creep or deviation from the work plan;
- Planned activities for the next reporting period;
- Gantt chart updated from the original to show actual progress; as applicable, explanations for variances and plan for completion on schedule;
- An accounting report for the current reporting period and a cumulative summary of the totals for both the current and previous reporting periods. The accounting report will include amounts invoiced to date and paid to date and a forecast of remaining budget and expenditures.

The Contractor’s point of contact for issue escalation from the State will be the Vice President of Applied Information Management. The State will assign a State Project Manager to oversee the coordination of tasks and advise the Contractor of acceptance of deliverables. The Blueprint Data Management/Analyst will serve in this capacity.

State resources will be sought out and staffed as required, and may impact the current schedule if not readily available. The success of this project is contingent upon both the State and the Contractor reasonably performing their respective responsibilities and completing their deliverables as assigned. The State Project Manager for this contract will:

- Ensure requirements are collected and documented;
- Ensure contractor deliverables are signed off by business;
- Track defects and turnaround times so that any necessary escalation may occur, and penalties are substantiated and invoked;
- Validate and approve contractor invoices submitted;
- Track issues and risks and escalate as needed;
- Track changes (Change Control) and State Communications required (Change Management);
- Host periodic stakeholder meetings, and publish stakeholder status reports.

The Contractor, in collaboration with the State Project Manager and State staff, will review for final acceptance each deliverable after date completed.

Deliverable: Full annual project plan and bi-weekly status reports

Task 7: Develop a Vermont Blueprint for Health Web Mapping and Data Analysis Plan

The Contractor will develop a data analysis and web mapping plan for the State. This plan will be for a system that will help the State understand progress in meeting program goals and in educating the public and monitoring progress of its activities over time. The plan will detail the areas of analysis based on interviews with State staff.

The Contractor will deliver a report to the State detailing the progress, activities, and analysis performed, as well as an outline of future goals and direction. This report needs to be presented in a format and language that is understandable and actionable for Blueprint staff and stakeholders (project managers, etc.). The report will also include mapping and examples of interactive features. The State Project Manager (Blueprint Data Management/Analyst) needs to approve and sign off on the plan/report.

Deliverables: Blueprint Data Analysis and Web Mapping plan

<u>Yearly Recurring Costs</u>

Task 8: Quarterly Penetration Testing

The Contractor will have a third party perform methodology-based, such as Open Source Security Testing Methodology (OSSTM), penetration testing quarterly and will provide results of that testing to the State. This budget assumes testing will be conducted once the application is in production with 2 pen-tests budgeted for the first year. Each pen-test consists of 2 days of testing. The price includes the cost of the 3rd party contractor to conduct the testing and time for the Contractor to work with the 3rd party contractor and report results back to the State. The

Contractor will notify the State in advance with the name of the 3rd party contractor doing the testing and when testing will occur. Upon completion of penetration tests, the Contractor will contact the AHS Security Director, via email to provide notification of each report. Notification will be provided to the State within 30 days of the penetration test being conducted. The Contractor and the AHS Security Director will then agree upon a secure delivery mode for the report and discuss the outcomes and recommendations of each scan together.

Deliverable: Quarterly penetration testing and securely delivered report results

Task 9: Hosting

The Contractor will provide ongoing support for the application once it is in use by the State staff and other user staff. The Contractor will host the State's solution within the United States of America using Amazon's Cloud solution as the hosting environment. Amazon will be a subcontractor of the Contractor for this purpose, and, as such, the Contractor agrees to accept all liability for the hosting agreement with Amazon. The service level agreement (SLA) for Amazon's hosting environment can be found at the following links:

- http://aws.amazon.com/ec2-sla/
- http://aws.amazon.com/articles/1697?_encoding=UTF8&jiveRedirect=1

The Contractor shall give the State not less than thirty (30) days advance written notice of any change to the Contractor's agreement with Amazon Cloud and/or change to where the State's system is being hosted. The State may terminate this contract if it determines, in its sole discretion, that such change is not in the best interest of the State.

Further, the State shall have the option, in its sole discretion, of selecting an alternative hosting provider. It shall give the Contractor not less than 90 days' notice of its desire to do so and shall provide the Contractor the reasonable cooperation required for such a transition.

Any third-party hosting environment on which the State's system is hosted shall meet the requirements of this Contract. The State shall have no direct contractual relationship with the hosting provider, nor any obligation to manage the Contractor's relationship with a hosting provider. Requirements herein for State access to the hosting platform shall be for compliance monitoring purposes only and shall in no way relieve the Contractor of its obligations with respect to managing its agreement with the hosting provider or in meeting the requirements of this Contract.

The application will be available for use at all times with the exception of planned service and maintenance, which must occur outside of normal business hours. For this application, the State defines normal business hours as 8 a.m. through 6 p.m. EST Monday through Friday.

The Contractor will strive to obtain a goal of 99.5% uptime yearly for the application. If at any time during the contract period the application site experiences downtime, with the exception of planned downtime for servicing, the State will be reimbursed at a rate of $0.75/hour (calculated

by cost of hosting/hours in a year) of downtime.

Before going live into production mode, the Contractor shall provide the State a disaster recovery plan and contingency plans for client lookup capabilities and online collaboration in the event of a disaster.

In the event of technical failure, such as a server going down, service shall be restored within 24 hours. In the event of a catastrophic event, the Contractor shall make every effort to restore service within 72 hours, assuming it is possible to do so. (For example, an extended East Coast power outage might prevent restoration from occurring within this timeframe.)

The Contractor will review patches and updates provided by the manufacturers of the software systems on the server used to fulfill the obligations of this contract to identify and implement patches and updates that should be applied to the server. This review will be done weekly at a minimum. Critical security patches and updates will always be immediately applied.

The cost is based on a monthly hosting fee of $300/month.

Deliverable: Disaster recovery plan; Monthly application hosting, and patching

Task 10: Technical Support and Application Maintenance (Change Requests)

The State has budgeted up to 12 hours per month of change requests, such as new data fields, new validation requests, and adding values to dropdown lists (outside of the original design), at a maximum hourly rate of $125/hour. Additionally, the State has budgeted up to four (4) hours per month of technical support to respond to user questions, at a maximum hourly rate of $125/hour. The State reserves the right to use all, some, or none of this budgeted monthly change request and technical support allotment and will be invoiced on a per use basis.

Deliverable: Monthly application maintenance (change requests) and technical support.

In addition to the tasks and ongoing maintenance listed above, the Contractor agrees to the following:

Web Services and SOA
The delivered solution will also include web services capabilities that will allow for it to function within a service-oriented architecture (SOA) environment. Services that are available to be exposed and consumed will be outlined in the solution's technical documentation.

Vendor Support

The Contractor will provide a complete description of their standard support offerings for end users and technical staff, including help desk, application, technical support, and standard service level agreement covering these services. This information will be provided to the State by the Contractor upon execution of the contract.

Documentation

Additional documentation requirements are outlined in the Custom Software section below.

The Contractor will provide manual(s) for the final product if it requires any interactions that must transpire with State employees, users external to the State Network, and/or external systems.

The Contractor will provide an installation manual for any product that is expected to be deployed onto State-owned equipment. The installation manual will clearly identify all necessary files, objects, and permissions needed to have the product deployed successfully.

Custom Software

The State shall solely own any custom software, including, but not limited to, application modules developed to integrate with a COTS product, source-codes, maintenance updates, documentation, training materials, and configuration files developed under any scope of work (SOW). Custom software developed for the State shall not be reused, resold, re-licensed, or repurposed by a vendor without written permission from an authorized representative of the State of Vermont CIO.

Upon the Contractor's voluntary or involuntary filing of bankruptcy or any other insolvency proceeding, Contractor's dissolution, Contractor's merger with or acquisition by another company or contractor, or discontinuance of support of any software or system, the Contractor shall convey to the State all rights, title, and interests in all custom software, software source codes, and all associated Software Source Code Documentation. For all custom software provided to the State pursuant to this contract, the Contractor shall either provide the source code directly to the State in a form acceptable to the State or deliver two copies of each software source code and Software Source Code Documentation to a State-approved escrow agent.

Data

- Data and derived data products (including aggregated, "de-identified", or "randomized" data) collected, manipulated, or directly purchased as part of a SOW shall become the exclusive property of the State. The State is considered the custodian of the data and shall determine the use, access, distribution, and other conditions based on appropriate State statutes and regulations.

- Licensed and/or copyrighted data shall be governed by the terms and conditions identified in the terms of agreement or the license.

- The Contractor, within one day of discovery, shall report to the State any security breach. The Contractor's report shall identify: (i) the nature of the security breach, (ii) the State Data used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure, (iv) what the Contractor has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action the Contractor has taken or shall take to prevent future similar unauthorized use or disclosure. The Contractor shall provide such other information, including a written report, as reasonably requested by the State.

- The Contractor agrees to comply with all applicable laws that require the notification of individuals in the event of unauthorized release of personally-identifiable information (PII),

including, but not limited to, Chapter 62 of Title 9 of the Vermont Statutes or other event requiring notification. In the event of a breach of any of the Contractor's security obligations or other event requiring notification under applicable law ("Notification Event"), the Contractor agrees to assume responsibility for informing all such individuals in accordance with applicable law.

- The Contractor will make every attempt to ensure any databases are SQL Server 2008 R2 and Oracle 11g compatible.

- In the event of a major incident, the application may lose no more than the last 24 hours of production data. (Recovery Point Objective).

- The Contractor shall provide the ability to recover from data loss due to end user error and end application error.

- The Contractor shall provide protection to maintain the integrity of data during concurrent access.

Encryption

The Contractor will address encryption requirements as follows:

1. All personally identifiable information (PII) data must be encrypted and must not impact program functionality, to include data at rest and data in motion, particularly when the State is not in physical control of the data.
2. Additional program data, as determined by the data owner, may be encrypted.
3. Data encryption methods may encompass cell-level, table-level, database-level, or file-level encryption, as long as objectives 1 and 2 are met. Additionally, all applications, Application Programming Interfaces (API), and services must be able to consume the data successfully using the selected method of encryption.
4. Encryption must use cryptographic key hierarchy conventions or its equivalent.
5. For encryption level, no encryption and simple encryption are unacceptable. Data Encryption Standard (DES) is acceptable, as long as the data resides within the State network at all times. Advanced Encryption Standard (AES) with keys of at least 128 bit blocks is preferred.

Backups

The Contractor will provide the ability to perform archival (full backup)/incremental (changed or new since last backup) backups and the ability to perform open/closed database backups.

The Contractor will establish a maintenance routine that will perform daily, weekly, and monthly backups, including tape rotation.

Full daily backups must be taken, unless the database is very large. In the event of a large database, full weekly backups and daily differential backups must be taken.

Database backup files must not be stored on the same subsystem as the primary database files. Separate storage is necessary.

A backup copy of the database will be moved to the Contractor's offices from the production server on a weekly basis.

The Contractor shall use offsite storage within the United States of America. Data backup should be housed offsite in a secure/fireproof vault or safe, in the event of a physical disaster.

A virtual machine snapshot will be taken periodically and following any major change to the production environment.

State Ownership of Data and Portability Following Contract Termination

The State's information, or any derivatives thereof, contained in any Contractor-owned repository (the "State Data," which shall also be known and treated by Contractor as Confidential Information) shall be and remain the sole and exclusive property of the State. The State shall be entitled to an export of State Data, without charge, upon the request of the State and upon termination of this Agreement. Following the termination of this Contract, the State will retain ownership of all database information, including specific client-level data and aggregate data sets.

The Contractor agrees to deliver all data to the State upon the State's request, and the Contractor will possess no lien or other such rights to the data. Data transfer, storage, and retrieval procedures must protect the original data from alteration. The data shall be delivered in a standard, agreed-upon format by the Contractor for the full range of customer data and will be transmitted to the State through secure means.

The State will have up to six (6) months of full access to State data (client-level data and aggregate data sets) to obtain downloads of all data to a container within the Vermont Agency of Human Services system or another hosted solution before the Contractor can destroy client-level data and aggregate data sets. Once the State has acknowledged in writing to the Contractor's legally appointed representative that all data have been downloaded, the Contractor will destroy all State data and supply the State with a certified affidavit that all data, including backups, have been destroyed in accordance with privacy and security standards.

In the event that the Contractor goes out of business before the end of this agreement, the Contractor agrees to deliver all data to the State upon the State's request, and the Contractor will possess no lien or other such rights to the data. Data transfer, storage, and retrieval procedures must protect the original data from alteration. The data shall be delivered in a standard, agreed-upon format by the Contractor for the full range of customer data and will be transmitted to the State through secure means. The Contractor will ensure that data is not available to any other entities but the State.

Open Standards

The Contractor will clearly identify whether the solution is fully functional using Open Standards, and, if not, the Contractor solution must specifically identify any proprietary or closed specification standards for which they do not support as a fully functional open alternative.

Application and Database Architecture

The Contractor will provide a description of the application and database architecture of the

solution being implemented. This description will clearly indicate security and adherence to industry best practices for Contractor's architecture. The Contractor will include a diagram depicting specific machines and points of transitions.

The Contractor is responsible for ensuring no unsupervised access to production or test environments that reside on State-owned machines. Access to production environments will be allowed for new implementations under certain conditions with proper security measures as long as the environments are fully segregated administratively.

Required Project Policies, Guidelines and Methodologies

The Contractor shall comply with all applicable State security policies and adhere to all legal, statutory, and regulatory requirements, as determined by Vermont leadership. The Contractor shall implement security controls in accordance with all Federal and State security policy and regulations. The Contractor will be required to comply with all applicable laws, regulations, policies, standards, and guidelines affecting information technology projects, which may be created or changed periodically. It is the responsibility of the Contractor to insure adherence to and to remain abreast of new or revised laws, regulations, policies, standards, and guidelines affecting project execution. Agency-specific confidentiality and privacy policies, such as Health Insurance Portability and Accountability Act (HIPAA), may apply. These may include, but are not limited to:

- The State's Information Technology Policies & Procedures at: http://dii.vermont.gov/Policy_Central
- The State's Record Management Best Practice at: http://vermont-archives.org/records/standards/pdf/RecordsManagementBestPractice.pdf
- The State Information Security Best Practice Guideline at: http://vermont-archives.org/records/standards/pdf/InformationSecurityBestPractice_Eff.20090501.pdf
- The State Digital Imaging Guidelines at: http://vermont-archives.org/records/standards/pdf/ImagingGuideline2008.pdf
- The State File Formats Best Practice at: http://vermont-archives.org/records/standards/pdf/FileFormatsBestPractice_Eff.20071201.pdf
- The State File Formats Guideline at: http://vermont-archives.org/records/standards/pdf/FileFormatsGuideline2008.pdf
- The State Metadata Guideline at: http://vermont-archives.org/records/standards/pdf/MetadataGuideline2008.pdf

Hosted System Requirements

The State will have the right to review the Contractor's information security program prior to the commencement of services and from time to time during the term of this Agreement. During the performance of the services, on an ongoing basis from time to time and without notice, the State, at its own expense, will be entitled to perform, or to have performed, an on-site audit of the Contractor's information security program. In lieu of an on-site audit, upon request by the State, the Contractor agrees to complete, within forty-five (45 days) of receipt, an audit questionnaire provided by the State regarding the Contractor's information security program.

The Contractor will implement any required safeguards as identified by the State or information security program audits.

If the State determines it is needed, the Contractor will sign a confidentiality agreement.

The State reserves the right to periodically audit the Contractor application infrastructure to ensure physical and network infrastructure meets the configuration and security standards and is in adherence to relevant State policies governing the system. Non-intrusive network audits (basic port scans, etc.) may be done randomly, without prior notice. More intrusive network and physical audits may be conducted on or off site with 24 hours' notice.

Security events will be reported to the State. Security-related events include, but are not limited to:

- Evidence of unauthorized access to privileged accounts
- Evidence of unauthorized access to data

All security-related events on critical or sensitive systems must be logged and audit trails saved for one year.

The Contractor will have a third party perform methodology-based (such as OSSTM) penetration testing quarterly and be willing to provide results of that testing to the State.

Hosted systems will issue passwords using one of the following methods:

1. Require administration to give password over the phone after identifying the individual.
2. Set a temporary password and have user change it after.

The vendor shall adhere to the principle of "Fail Safe" to ensure that a system in a failed state does not reveal any sensitive information or leave any access controls open for attacks.

Dispute Resolution

The parties will seek a fair and prompt negotiated resolution within ten (10) business days of the initial notice of the dispute. If the dispute has not been resolved after such time, the parties will escalate the issue to more senior levels. Nothing herein shall prevent either party from seeking a preliminary or permanent injunction to prevent irreparable harm during the negotiation process or diminish the respective rights of the parties to pursue any and all remedies available in law and/or equity at any time. Should the dispute involve payment for requested services outside of the scope of the Agreement, in no event shall the Contractor be obligated to perform such services until the dispute has been resolved to the satisfaction of both parties.

ATTACHMENT B

PAYMENT PROVISIONS

The maximum dollar amount payable under this agreement is not intended as any form of a guaranteed amount. The Contractor will be paid for products or services actually performed as specified in Attachment A up to the maximum allowable amount specified in this agreement. State of Vermont payment terms are Net 30 days from date of invoice, payments against this contract will comply with the 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. Contractor invoices shall be submitted no more frequently than monthly, but no later than quarterly, and shall include the deliverables completed during the specified billing period and the total amount invoiced. The State shall pay the Contractor based on lump sum payments for each of the following deliverables, except where otherwise noted. Lump sum payments will only be made for deliverables accepted by the State.

   Contract Deliverable 1: Complete Database and Blueprint Web Application Design and Development completed by the date specified within the mutually agreed upon project plan, with payment of $4500 upon delivery and acceptance by the State.

   Contract Deliverable 2: Complete Database and Front End Forms completed by the date specified within the mutually agreed upon project plan, with payment of $33,000 upon delivery and acceptance by the State.

   Contract Deliverable 3: Develop Reporting System for Blueprint Database Application completed by the date specified within the mutually agreed upon project plan, with payment of $14,000 upon delivery and acceptance by the State.

   Contract Deliverable 4: User Testing, Acceptance, Application Refinement, and Deployment completed by the date specified within the mutually agreed upon project plan, with payment of $11,000 upon completion and acceptance by the State, including bug fixes.

   Contract Deliverable 5: Documentation and Training completed by the date specified within the mutually agreed upon project plan, with payment of $9,500 upon delivery and acceptance by the State.

   Contract Deliverable 6: Project management invoiced and paid monthly in 12 equal installments of $1500, totaling $18,000, based on delivery of a full project plan by July 30, 2013, subject to approval by the State, and delivery of bi-weekly status reports.

   Contract Deliverable 7: Develop a Vermont Blueprint for Health Web Mapping and Data Analysis Plan completed by the date specified within the mutually agreed upon project plan, with payment of $5,000 upon delivery and acceptance by the State.

In addition, the State shall pay recurring annual costs for the following:

Contract Deliverable 8: Quarterly Penetration Testing performed as an ongoing service after application is in production with payment of $8,250 in year one and $16,500 in year two.

Contract Deliverable 9: Hosting performed as an ongoing service after application is in production. For the first year, the Contractor shall provide hosting at no cost for the first 6 months with a monthly fee of $300 per month for the subsequent 6 months and the following 2 years, totaling $1,800 for the first year and $3,600 for the second and third years.

Contract Deliverable 10: Monthly Technical Support and Application Maintenance (Change Requests) performed as requested after application is in production. Based on the number of hours used monthly by the State for change requests, such as new data fields, new validation requests, and adding values to dropdown lists (outside of the original design), application maintenance will be paid at a maximum rate of $125 per hour with a maximum of 12 hours budgeted per month ($1500 per month maximum). The Contractor shall invoice the State only for actual application maintenance hours used each month. The Contractor will notify the State if change request work is scoped to exceed the 12 hour per month maximum. The State must approve any change request work which exceeds the monthly maximum prior to execution of said work. The maximum payment for year one shall not exceed $9,000. Annual payment for application maintenance (change requests) in the second year shall not exceed $18,000.

Additionally, the State has budgeted up to four (4) hours per month of technical support to respond to user questions, at a maximum hourly rate of $125/hour ($500 per month maximum). The maximum annual payment for year one shall not exceed $3,000 for technical support and shall not exceed $6,000 in the second year. The Contractor shall invoice the State only for actual technical support hours used each month. Such invoices shall detail the actual dates, description of service, and hours of services per incident.

The following table summarizes the maximum budget for year 1 and 2 costs:

Blueprint Application Budget Summary

Task	Description	Year 1	Year 2
Task 1	Complete Blueprint Application Design	$ 4,500	
Task 2	Complete Database and Front End Forms	$ 33,000	
Task 3	Develop Blueprint Reporting System	$ 14,000	
Task 4	User Testing, Acceptance, Application Refinement, and Deployment	$ 11,000	

Task 5	Documentation and Training	$ 9,500	
Task 6	Project Management	$ 18,000	
Task 7	Blueprint Data Analysis Plan	$ 5,000	
Subtotal		**$ 95,000**	
Task 8	Quarterly Penetration Testing	$ 8,250	$ 16,500
Task 9	Hosting and Technical Support	$ 1,800	$ 3,600
Task 10	Application Maintenance	$ 12,000	$ 24,000
Annual Cost		**$ 117,050**	**$ 44,100**

2. Before invoicing and payment commences, the Contractor will provide Craig Benson, Agency of Human Services (AHS) Data Services Director, with a completed/finalized Data Dictionary via email to Craig.Benson@state.vt.us, subject to State review and approval.

3. All work products (deliverables) are subject to review and approval by the State before being accepted, including but not limited to any individual Change Request resulting from Deliverable #10 above. Each work product will be evaluated based on any and all descriptions listed within Attachment A, as well as all direction and input discussed and agreed upon between the State and the Contractor during the term of this Agreement as it aligns with the specifications of work. Any work product deemed unacceptable by the State will be subject to revision by the Contractor based upon a remediation plan that the State and the Contractor will develop. Payment will be contingent upon the State accepting each work product and any stipulations listed above.

4. No benefits or insurance will be reimbursed by the State.

5. Invoices should reference this contract number and be submitted to:

   DVHA Business Office, Contracting Unit
   Department of Vermont Health Access
   312 Hurricane Lane, Suite 201
   Williston, VT 05495

6. The total maximum amount payable under this contract shall not exceed $161,150.

ATTACHMENT C
CUSTOMARY PROVISIONS FOR CONTRACTS AND GRANTS

1. **Entire Agreement.** This Agreement, whether in the form of a Contract, State Funded Grant, or Federally Funded Grant, represents the entire agreement between the parties on the subject matter. All prior agreements, representations, statements, negotiations, and understandings shall have no effect.

2. **Applicable Law.** This Agreement will be governed by the laws of the State of Vermont.

3. **Definitions:** For purposes of this Attachment, "Party" shall mean the Contractor, Grantee or Subrecipient, with whom the State of Vermont is executing this Agreement and consistent with the form of the Agreement.

4. **Appropriations:** If appropriations are insufficient to support this Agreement, the State may cancel on a date agreed to by the parties or upon the expiration or reduction of existing appropriation authority. In the case that this Agreement is funded in whole or in part by federal or other non-State funds, and in the event those funds become unavailable or reduced, the State may suspend or cancel this Agreement immediately, and the State shall have no obligation to fund this Agreement from State revenues.

5. **No Employee Benefits For Party:** The Party understands that the State will not provide any individual retirement benefits, group life insurance, group health and dental insurance, vacation or sick leave, workers compensation or other benefits or services available to State employees, nor will the state withhold any state or federal taxes except as required under applicable tax laws, which shall be determined in advance of execution of the Agreement. The Party understands that all tax returns required by the Internal Revenue Code and the State of Vermont, including but not limited to income, withholding, sales and use, and rooms and meals, must be filed by the Party, and information as to Agreement income will be provided by the State of Vermont to the Internal Revenue Service and the Vermont Department of Taxes.

6. **Independence, Liability:** The Party will act in an independent capacity and not as officers or employees of the State.

   The Party shall defend the State and its officers and employees against all claims or suits arising in whole or in part from any act or omission of the Party or of any agent of the Party. The State shall notify the Party in the event of any such claim or suit, and the Party shall immediately retain counsel and otherwise provide a complete defense against the entire claim or suit. The Party shall notify its insurance company and the State within 10 days of receiving any claim for damages, notice of claims, pre-claims, or service of judgments or claims, for any act or omissions in the performance of this Agreement.

   After a final judgment or settlement the Party may request recoupment of specific defense costs and may file suit in Washington Superior Court requesting recoupment. The Party shall be entitled to recoup costs only upon a showing that such costs were entirely unrelated to the defense of any claim arising from an act or omission of the Party.

   The Party shall indemnify the State and its officers and employees in the event that the State, its officers or employees become legally obligated to pay any damages or losses arising from

any act or omission of the Party.

7. **Insurance**: Before commencing work on this Agreement the Party must provide certificates of insurance to show that the following minimum coverage is in effect. It is the responsibility of the Party to maintain current certificates of insurance on file with the state through the term of the Agreement. No warranty is made that the coverage and limits listed herein are adequate to cover and protect the interests of the Party for the Party's operations. These are solely minimums that have been established to protect the interests of the State.

   Workers Compensation: With respect to all operations performed, the Party shall carry workers' compensation insurance in accordance with the laws of the State of Vermont.

   General Liability and Property Damage: With respect to all operations performed under the Agreement, the Party shall carry general liability insurance having all major divisions of coverage including, but not limited to:

   Premises - Operations
   Products and Completed Operations
   Personal Injury Liability
   Contractual Liability

   The policy shall be on an occurrence form and limits shall not be less than:

   $1,000,000 Per Occurrence
   $1,000,000 General Aggregate
   $1,000,000 Products/Completed Operations Aggregate
   $ 50,000 Fire/ Legal/Liability

   Party shall name the State of Vermont and its officers and employees as additional insureds for liability arising out of this Agreement.

   Automotive Liability: The Party shall carry automotive liability insurance covering all motor vehicles, including hired and non-owned coverage, used in connection with the Agreement. Limits of coverage shall not be less than: $1,000,000 combined single limit.

   Party shall name the State of Vermont and its officers and employees as additional insureds for liability arising out of this Agreement.

   Professional Liability*:** Before commencing work on this Agreement and throughout the term of this Agreement, the Party shall procure and maintain professional liability insurance for any and all services performed under this Agreement, with minimum coverage of ***$____NA____ per occurrence, and ***$____NA____*** aggregate.

8. **Reliance by the State on Representations:** All payments by the State under this Agreement will be made in reliance upon the accuracy of all prior representations by the Party, including but not limited to bills, invoices, progress reports and other proofs of work.

9. **Requirement to Have a Single Audit:** In the case that this Agreement is a Grant that is funded in whole or in part by federal funds, the Subrecipient will complete the Subrecipient Annual Report annually within 45 days after its fiscal year end, informing the State of

Vermont whether or not a single audit is required for the prior fiscal year. If a single audit is required, the Subrecipient will submit a copy of the audit report to the granting Party within 9 months. If a single audit is not required, only the Subrecipient Annual Report is required.

A single audit is required if the subrecipient expends $500,000 or more in federal assistance during its fiscal year and must be conducted in accordance with OMB Circular A-133. The Subrecipient Annual Report is required to be submitted within 45 days, whether or not a single audit is required.

10. **Records Available for Audit:** The Party will maintain all books, documents, payroll papers, accounting records and other evidence pertaining to costs incurred under this agreement and make them available at reasonable times during the period of the Agreement and for three years thereafter for inspection by any authorized representatives of the State or Federal Government. If any litigation, claim, or audit is started before the expiration of the three year period, the records shall be retained until all litigation, claims or audit findings involving the records have been resolved. The State, by any authorized representative, shall have the right at all reasonable times to inspect or otherwise evaluate the work performed or being performed under this Agreement.

11. **Fair Employment Practices and Americans with Disabilities Act**: Party agrees to comply with the requirement of Title 21V.S.A. Chapter 5, Subchapter 6, relating to fair employment practices, to the full extent applicable. Party shall also ensure, to the full extent required by the Americans with Disabilities Act of 1990, as amended, that qualified individuals with disabilities receive equitable access to the services, programs, and activities provided by the Party under this Agreement. Party further agrees to include this provision in all subcontracts.

12. **Set Off**: The State may set off any sums which the Party owes the State against any sums due the Party under this Agreement; provided, however, that any set off of amounts due the State of Vermont as taxes shall be in accordance with the procedures more specifically provided hereinafter.

13. **Taxes Due to the State**:

    a. Party understands and acknowledges responsibility, if applicable, for compliance with State tax laws, including income tax withholding for employees performing services within the State, payment of use tax on property used within the State, corporate and/or personal income tax on income earned within the State.

    b. Party certifies under the pains and penalties of perjury that, as of the date the Agreement is signed, the Party 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.

    c. Party understands that final payment under this Agreement may be withheld if the Commissioner of Taxes determines that the Party is not in good standing with respect to or in full compliance with a plan to pay any and all taxes due to the State of Vermont.

    d. Party also understands the State may set off taxes (and related penalties, interest and fees) due to the State of Vermont, but only if the Party has failed to make an appeal

within the time allowed by law, or an appeal has been taken and finally determined and the Party has no further legal recourse to contest the amounts due.

14. Child Support: (Applicable if the Party is a natural person, not a corporation or partnership.) Party states that, as of the date the Agreement is signed, he/she:

a. is not under any obligation to pay child support; or
b. is under such an obligation and is in good standing with respect to that obligation; or
c. has agreed to a payment plan with the Vermont Office of Child Support Services and is in full compliance with that plan.

Party makes this statement with regard to support owed to any and all children residing in Vermont. In addition, if the Party is a resident of Vermont, Party makes this statement with regard to support owed to any and all children residing in any other state or territory of the United States.

15. Sub-Agreements: Party shall not assign, subcontract or subgrant the performance of his Agreement or any portion thereof to any other Party without the prior written approval of the State. Party also agrees to include in subcontract or subgrant agreements a tax certification in accordance with paragraph 13 above.

Notwithstanding the foregoing, the State agrees that the Party may assign this agreement, including all of the Party's rights and obligations hereunder, to any successor in interest to the Party arising out of the sale of or reorganization of the Party.

16. No Gifts or Gratuities: Party shall not give title or possession of any thing of substantial value (including property, currency, travel and/or education programs) to any officer or employee of the State during the term of this Agreement.

17. Copies: All written reports prepared under this Agreement will be printed using both sides of the paper.

18. Certification Regarding Debarment: Party certifies under pains and penalties of perjury that, as of the date that this Agreement is signed, neither Party nor Party'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.

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

19. Certification Regarding Use of State Funds: In the case that Party is an employer and this Agreement is a State Funded Grant in excess of $1,001, Party certifies that none of these State funds will be used to interfere with or restrain the exercise of Party's employee's rights with respect to unionization.

Attachment E
BUSINESS ASSOCIATE AGREEMENT

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 Stone Environmental, Inc. ("Business Associate") as of **July 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 binds 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 identify in writing upon request from Covered Entity all of the safeguards that it uses to prevent impermissible uses or disclosures of PHI.

5. **Documenting and Reporting Breaches**.

5.1 Business Associate shall report to Covered Entity any Breach of Unsecured PHI as soon as it (or any of its employees or agents) become aware of any such Breach, and in no case later than three (3) business days after it (or any of its employees or agents) 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 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 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 provide notice to the individuals whose PHI was the subject of the Breach. 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.

9. **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 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, 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 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 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 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 Business Associate breaches any material term of this Agreement, Covered Entity may either: (a) provide
an opportunity for Business Associate to cure the breach and Covered Entity may terminate this Contract without liability or penalty if Business Associate does not cure the breach within the time specified by Covered Entity; or (b) immediately terminate this Contract without liability or penalty if Covered Entity believes that cure is not reasonably possible; or (c) if neither termination nor cure are feasible, Covered Entity shall report the breach to the Secretary. Covered Entity has the right to seek to cure any breach by Business Associate and this right, regardless of whether Covered Entity cures such breach, does not lessen any right or remedy available to Covered Entity at law, in equity, or under this Contract, nor does it lessen Business Associate's responsibility for such breach or its duty to cure such breach.

14. Return/Destruction of PHI.

14.1 Business Associate in connection with the expiration or termination of this Contract shall return or destroy 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.

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 identify in writing upon request from Covered Entity all of the safeguards that it uses to protect such Electronic PHI.

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.

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.

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

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 Covered Entity to comply with the Privacy Rule, the Security Rule, or any other standards promulgated under HIPAA.

17.3 Any ambiguity in this Agreement shall be resolved to permit Covered Entity to

comply with the Privacy Rule, Security Rule, or any other standards promulgated under HIPAA.

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 with respect to accounting requests, if any, made after such expiration or termination.

ATTACHMENT F
AGENCY OF HUMAN SERVICES' CUSTOMARY CONTRACT PROVISIONS

1. **Agency of Human Services - Field Services Directors** will share oversight with the department (or field office) that is a party to the contract for provider performance using outcomes, processes, terms and conditions agreed to under this contract.

2. **2-1-1 Data Base:** The Contractor providing a health or human services within Vermont, or near the border that is readily accessible to residents of Vermont, will provide relevant descriptive information regarding its agency, programs and/or contact and will adhere to the "Inclusion/Exclusion" policy of Vermont's United Way/Vermont 211. If included, the Contractor will provide accurate and up to date information to their data base as needed. The "Inclusion/Exclusion" policy can be found at www.vermont211.org

3. **Medicaid Program Contractors**:
Inspection of Records: Any contracts accessing payments for services through the Global Commitment to Health Waiver and Vermont Medicaid program must fulfill state and federal legal requirements to enable the Agency of Human Services (AHS), the United States Department of Health and Human Services (DHHS) and the Government Accounting Office (GAO) to:

   Evaluate through inspection or other means the quality, appropriateness, and timeliness of services performed; and Inspect and audit any financial records of such Contractor or subcontractor.

   Subcontracting for Medicaid Services: Having a subcontract does not terminate the Contractor, receiving funds under Vermont's Medicaid program, from its responsibility to ensure that all activities under this agreement are carried out. Subcontracts must specify the activities and reporting responsibilities of the Contractor or subcontractor and provide for revoking delegation or imposing other sanctions if the Contractor or subcontractor's performance is inadequate. The Contractor agrees to make available upon request to the Agency of Human Services; the Department of Vermont Health Access; the Department of Disabilities, Aging and Independent Living; and the Center for Medicare and Medicaid Services (CMS) all contracts and subcontracts between the Contractor and service providers.

   Medicaid Notification of Termination Requirements: Any Contractor accessing payments for services under the Global Commitment to Health Waiver and Medicaid programs who terminates their practice will follow the Department of Vermont Health Access, Managed Care Organization enrollee notification requirements.

   Encounter Data: Any Contractor accessing payments for services through the Global Commitment to Health Waiver and Vermont Medicaid programs must provide encounter data to the Agency of Human Services and/or its departments and ensure that it can be linked to enrollee eligibility files maintained by the State.

   Federal Medicaid System Security Requirements Compliance: All contractors and subcontractors must provide a security plan, risk assessment, and security controls review document within three months of the start date of this agreement (and update it annually thereafter) to support audit compliance with 45CFR95.621 subpart F, *ADP* (Automated Data Processing) *System Security Requirements and Review Process*.

4. **Non-discrimination Based on National Origin as evidenced by Limited English Proficiency**. The Contractor agrees to comply with the non-discrimination requirements of Title VI of the Civil Rights Act of 1964, 42 USC Section 2000d, et seq., and with the federal guidelines promulgated pursuant to Executive Order 13166 of 2000, which require that contractors and subcontractors receiving federal funds must assure that persons with limited English proficiency can meaningfully access services. To the extent the Contractor provides assistance to individuals with limited English proficiency through the use of oral or written translation or interpretive services in compliance with this requirement, such individuals cannot be required to pay for such services.

5. **Voter Registration**. When designated by the Secretary of State, the Contractor agrees to become a voter registration agency as defined by 17 V.S.A. §2103 (41), and to comply with the requirements of state and federal law pertaining to such agencies.

6. **Drug Free Workplace Act.** The Contractor will assure a drug-free workplace in accordance with 45 CFR Part 76.

7. **Privacy and Security Standards.**

   Protected Health Information: The Contractor shall maintain the privacy and security of all individually identifiable health information acquired by or provided to it as a part of the performance of this contract. The Contractor shall follow federal and state law relating to privacy and security of individually identifiable health information as applicable, including the Health Insurance Portability and Accountability Act (HIPAA) and its federal regulations.

   Substance Abuse Treatment Information: The confidentiality of any alcohol and drug abuse treatment information acquired by or provided to the Contractor or subcontractor shall be maintained in compliance with any applicable state or federal laws or regulations and specifically set out in 42 CFR Part 2.

   Other Confidential Consumer Information: The Contractor agrees to comply with the requirements of AHS Rule No. 08-048 concerning access to information. The Contractor agrees to comply with any applicable Vermont State Statute, including but not limited to 12 VSA §1612 and any applicable Board of Health confidentiality regulations. The Contractor shall ensure that all of its employees and subcontractors performing services under this agreement understand the sensitive nature of the information that they may have access to and sign an affirmation of understanding regarding the information's confidential and non-public nature.

   Social Security numbers: The Contractor agrees to comply with all applicable Vermont State Statutes to assure protection and security of personal information, including protection from identity theft as outlined in Title 9, Vermont Statutes Annotated, Ch. 62.

8. **Abuse Registry.** The Contractor agrees not to employ any individual, use any volunteer, or otherwise provide reimbursement to any individual in the performance of services connected with this agreement, who provides care, custody, treatment, transportation, or supervision to children or vulnerable adults if there is a substantiation of abuse or neglect or exploitation against that individual. The Contractor will check the Adult Abuse Registry in the Department of Disabilities, Aging and Independent Living. Unless the Contractor holds a valid child care license or registration from the Division of Child Development, Department for Children and

Families, the Contractor shall also check the Central Child Protection Registry. (See 33 V.S.A. §4919(a)(3) & 33 V.S.A. §6911(c)(3)).

9. **Reporting of Abuse, Neglect, or Exploitation.** Consistent with provisions of 33 V.S.A. §4913(a) and §6903, any agent or employee of a Contractor who, in the performance of services connected with this agreement, has contact with clients or is a caregiver and who has reasonable cause to believe that a child or vulnerable adult has been abused or neglected as defined in Chapter 49 or abused, neglected, or exploited as defined in Chapter 69 of Title 33 V.S.A. shall make a report involving children to the Commissioner of the Department for Children and Families within 24 hours or a report involving vulnerable adults to the Division of Licensing and Protection at the Department of Disabilities, Aging, and Independent Living within 48 hours. This requirement applies except in those instances where particular roles and functions are exempt from reporting under state and federal law. Reports involving children shall contain the information required by 33 V.S.A. §4914. Reports involving vulnerable adults shall contain the information required by 33 V.S.A. §6904. The Contractor will ensure that its agents or employees receive training on the reporting of abuse or neglect to children and abuse, neglect or exploitation of vulnerable adults.

10. **Intellectual Property/Work Product Ownership.** All data, technical information, materials first gathered, originated, developed, prepared, or obtained as a condition of this agreement and used in the performance of this agreement - including, but not limited to all reports, surveys, plans, charts, literature, brochures, mailings, recordings (video or audio**)**, pictures, drawings, analyses, graphic representations, software computer programs and accompanying documentation and printouts, notes and memoranda, written procedures and documents, which are prepared for or obtained specifically for this agreement - or are a result of the services required under this grant - shall be considered "work for hire" and remain the property of the State of Vermont, regardless of the state of completion - unless otherwise specified in this agreement. Such items shall be delivered to the State of Vermont upon 30 days' notice by the State. With respect to software computer programs and / or source codes first developed for the State, all the work shall be considered "work for hire," i.e., the State, not the Contractor or subcontractor, shall have full and complete ownership of all software computer programs, documentation and/or source codes developed.

    The Contractor shall not sell or copyright a work product or item produced under this agreement without explicit permission from the State.

    If the Contractor is operating a system or application on behalf of the State of Vermont, then the Contractor shall not make information entered into the system or application available for uses by any other party than the State of Vermont, without prior authorization by the State. Nothing herein shall entitle the State to pre-existing Contractor's materials.

11. **Security and Data Transfers.** The State shall work with the Contractor to ensure compliance with all applicable State and Agency of Human Services' policies and standards, especially those related to privacy and security. The State will advise the Contractor of any new policies, procedures, or protocols developed during the term of this agreement as they are issued and will work with the Contractor to implement any required.

    The Contractor will ensure the physical and data security associated with computer equipment - including desktops, notebooks, and other portable devices - used in connection

with this agreement. The Contractor will also assure that any media or mechanism used to store or transfer data to or from the State includes industry standard security mechanisms such as continually up-to-date malware protection and encryption. The Contractor will make every reasonable effort to ensure media or data files transferred to the State are virus and spyware free. At the conclusion of this agreement and after successful delivery of the data to the State, the Contractor shall securely delete data (including archival backups) from the Contractor's equipment that contains individually identifiable records, in accordance with standards adopted by the Agency of Human Services.

12. **Computing and Communication:** The Contractor shall select, in consultation with the Agency of Human Services' Information Technology unit, one of the approved methods for secure access to the State's systems and data, if required. Approved methods are based on the type of work performed by the Contractor as part of this agreement. Options include, but are not limited to:

    1. Contractor's provision of certified computing equipment, peripherals and mobile devices, on a separate Contractor's network with separate internet access. The Agency of Human Services' accounts may or may not be provided.

    2. State supplied and managed equipment and accounts to access state applications and data, including State issued active directory accounts and application specific accounts, which follow the National Institutes of Standards and Technology (NIST) security and the Health Insurance Portability & Accountability Act (HIPAA) standards.

    The State will not supply e-mail accounts to the Contractor.

13. **Lobbying.** No federal funds under this agreement may be used to influence or attempt to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with the awarding of any federal contract, continuation, renewal, amendments other than federal appropriated funds.

14. **Non–discrimination.** The Contractor will prohibit discrimination on the basis of age under the Age Discrimination Act of 1975, on the basis of handicap under section 504 of the Rehabilitation Act of 1973, on the basis of sex under Title IX of the Education Amendments of 1972, or on the basis of race, color or national origin under Title VI of the Civil Rights Act of 1964. No person shall on the grounds of sex (including, in the case of a woman, on the grounds that the woman is pregnant) or on the grounds of religion, be excluded from participation in, be denied the benefits of, or be subjected to discrimination, to include sexual harassment, under any program or activity supported by state and/or federal funds.

    The Contractor will also not refuse, withhold from or deny to any person the benefit of services, facilities, goods, privileges, advantages, or benefits of public accommodation on the basis of disability, race, creed, color, national origin, marital status, sex, sexual orientation or gender identity under Title 9 V.S.A. Chapter 139.

15. **Environmental Tobacco Smoke.** Public Law 103-227, also known as the Pro-children Act of 1994 (Act), requires that smoking not be permitted in any portion of any indoor facility owned or leased or contracted for by an entity and used routinely or regularly for the provision of health, child care, early childhood development services, education or library

services to children under the age of 18, if the services are funded by federal programs either directly or through state or local governments, by federal grant, contract, loan or loan guarantee. The law also applies to children's services that are provided in indoor facilities that are constructed, operated, or maintained with such Federal funds.

The law does not apply to children's services provided in private residences; portions of facilities used for inpatient drug or alcohol treatment; service providers whose sole source of applicable federal funds is Medicare or Medicaid; or facilities where Women, Infants, & Children (WIC) coupons are redeemed.

Failure to comply with the provisions of the law may result in the imposition of a civil monetary penalty of up to $1,000 for each violation and/or the imposition of an administrative compliance order on the responsible entity.

Contractors are prohibited from promoting the use of tobacco products for all clients. Facilities supported by state and federal funds are prohibited from making tobacco products available to minors.

ATTACHMENT G

SPECIFICATIONS OF WORK PERFORMED FROM ORIGINAL CONTRACT

General Conditions
The Contractor will develop a prototype of a web accessible database application that will allow practices, project managers, and State staff to easily enter, track, and report on Blueprint practice, provider and community health team data.

All users will be provided with a secure username and password, and each user will be assigned to a role that allows for a specific level of activity. Upon logging into the application, there will be various options for entering data. The application will contain multiple forms based on sheets currently contained in the "Readiness Database" Excel workbook maintained by the State.

Project tasks are as follows:

Task 1: Project Start-up and initial Project Communication
The Contractor will receive final templates from the State. The State will be responsible for identifying which fields in the templates should be included in the database application.

Task 2: Application Mock-up
The application and forms will be mocked-up using Protoshare, which is an online prototyping application that allows users to rapidly create a mock-up of the application for review without writing any code. The mock-up will include the general layout and navigation of the site and each of the individual data entry forms. Once the mock-up is complete, the State can provide feedback and suggested changes. This process will ensure that State staff is comfortable with the look and feel of the application prior to actual development.

Task 3: Application Development
Includes the setup of the application framework (server set up, database design and implementation of user security), and the creation of user interface (built in Visual Studio 2010). The layout and navigation of the application and the individual forms will be based on the mock-up established in Protoshare. The application will contain the following forms: User Administration Form, Health Service Area Form, Practice Form, Provider Form, Community Health Team Form, and Community Health Team (CHT) Staffing Form. Each of the data entry forms will contain the following functionality: add new record, edit record, delete record

Task 4: Simple Data Extraction Tool
The simple data extraction tool will contain a form which will allow users to extract data to CSV file format (compatible with Excel) for further filtering. Users will only be allowed to download data that they have permission to view based on their role. The tool will have four options: download practice data, download provider data, download CHT data, and download CHT staffing data.

Task 5: Data Upload
Data contained in the Readiness Database Excel workbook will be used to populate the backend SQL database for the application. Two data uploads have been budgeted. The first data upload

will allow the State to have data to work with in order to complete testing during application development. Throughout this first upload, scripts will be written to automate subsequent uploads. The final upload will occur prior to application deployment, and it will be done with the most current version of the Blueprint readiness database. The data upload will include the following worksheets from the Readiness Database Excel workbook: Practices, Providers, CHT Administrative Entity, CHT Staff Names and other worksheets identified by the State Blueprint staff during project startup will also be uploaded to the database.

Task 6: User Testing, Acceptance and Application Refinement
Upon completion of the prototype application, the State will test all aspects of the application to ensure that it meets initial requirements. Stone will respond to bug fixes within this scope of effort. The State may provide Stone with a list of changes that would further refine needs beyond this work scope and request a cost estimate for those enhancements.

Hosting
In addition to the tasks above, the Contractor will host the application at no cost for the first six months of the project.