



## ADDENDUM #2

### RFP-2017-DPHS-03-CANCE

On July 15, 2016, the New Hampshire Department of Health and Human Services published a request to solicit applications from vendors to operate an incidence-based statewide cancer registry system to collect statewide data on new cancer cases diagnosed among New Hampshire residents and conduct data collection, data processing, quality assurance and database management activities.

The Department is publishing this addendum to:

#### **3.1. Covered Populations and Services**

**Delete 3.1.**

**Replace with:**

#### **3.1. Covered Populations and Services**

The area served is statewide. The Contractor will conduct statewide cancer data collection, data processing, quality assurance and database management activities for the New Hampshire State Cancer Registry in accordance with NH DHHS, RSA 141-B, He-P 304 NH administrative rules ([http://www.gencourt.state.nh.us/rules/state\\_agencies/he-p300.html](http://www.gencourt.state.nh.us/rules/state_agencies/he-p300.html)), United States Public Law 102-515 (<http://www.cdc.gov/cancer/npcr/pdf/publaw.pdf>) and guidelines and standards set by National Program for Cancer Registry (NPCR) ([http://www.cdc.gov/cancer/npcr/pdf/npcr\\_standards.pdf](http://www.cdc.gov/cancer/npcr/pdf/npcr_standards.pdf)) and the North American Association of Central Cancer Registries (NAACCR) (<http://naaccr.org/StandardsandRegistryOperations/Volumell.aspx>).

Activities will be conducted in a manner designed to complement activities performed by DHHS, resulting in seamless integration between contractor activities and NHSCR operations. The Contractor shall provide web-based connectivity for database users, provide database management expertise and technical services, conduct quality assurance/quality control activities, provide system security, and provide all means sufficient to complete the requirements listed in the Statement of Work.

#### **3.2. Cancer Registry Operation Required Services**

**Delete 3.2.1.**

**Replace with:**

- 3.2.1.** Operate an incidence-based statewide cancer registry reporting system in accordance with RSA 141-B and Part He-P 304.0 of the New Hampshire Administrative Rules ([http://www.gencourt.state.nh.us/rules/state\\_agencies/he-p300.html](http://www.gencourt.state.nh.us/rules/state_agencies/he-p300.html)). Collect information and maintain an electronic database of all incident cancer cases occurring among the New Hampshire population according to the Administrative Rules.



## New Hampshire Department of Health and Human Services Cancer Registry Operations

- 3.2.2. Facilitate and encourage submission of reports for each incident case defined in RSA 141-B:7 (<http://www.gencourt.state.nh.us/rsa/html/X/141-B/141-B-mrg.htm>), all the data variables listed in administrative rule He-P 304.02 by “health facilities” within an expected time frame as listed in Administrative Rule He-P 304.01(e) and He-P 304.01(l) ([http://www.gencourt.state.nh.us/rules/state\\_agencies/he-p300.html](http://www.gencourt.state.nh.us/rules/state_agencies/he-p300.html)). Facilitation and encouragement may include writing letters, calling by telephone and personal visits to health providers and/or health facility administrators or supervisors. (“Health Facilities” shall be defined according to Administrative Rules.)

### 3.5. Information Technology Activities

**Delete 3.5. Information Technology Activities**  
**Replace with:**

### 3.5. Information Technology Activities

- 3.5.1. Establish operations within 30 days of the contract start date. This shall include, but not be limited to system set-up, testing, and deployment, as well as business operations to support the State’s requirements defined in Appendix F – Cancer Data Registry Technical Requirements.
- 3.5.2. Within 30 days of the contract start date, provide and set up necessary computer hardware, including servers and computers for the NHSCR contractor staff, necessary to maintain the NHSCR database. All hardware and software shall be compatible with NPCR requirements.
- 3.5.3. Within 30 days of the contract start date, provide connectivity for all reporting facilities to transmit data to the NHCSR.
- 3.5.4. Within 30 days of the contract start date, provide connectivity for all reporting facilities to the NHCSR database on secure server.
- 3.5.5. Maintain secure web access to the NHSCR seven days per week for Web Plus on-line data entry and data file uploading.
- 3.5.6. Within 30 days of the contract start date, obtain from the prior NHSCR vendor a copy of the latest version of the confidential NHSCR database, and copies of hard copy logs and electronic logs of abstracts submitted to the NHSCR.
- 3.5.7. Within 30 days of the contract start date, install and utilize the current automated data management system, consistent with national standards and populated with NHSCR data. Train staff in operation of software systems. The contractor shall update all the components of the software, as required and shall participate in the relevant CDC software users group. (The DHHS maintains the discretion to utilize any kind of data management system. There shall be no modifications or upgrades to the software without the approval of the DHHS.)
- 3.5.8. Restrict reporting via Web Plus data entry or file upload to those reporters who have submitted signed agreements to become Web Plus users. .
- 3.5.9. Within 30 days of the contract start date, develop and implement procedures for the electronic submission and processing of laboratory pathology and cytology reports utilizing NAACCR standards.



## New Hampshire Department of Health and Human Services Cancer Registry Operations

---

- 3.5.10. Within 30 days of the contract start date, maintain a computerized log of facilities and personnel who report data to NHSCR (in excel or access or any other system) which includes at minimum; facility ID, name and demographic information; names and contact information of personnel (reporters and supervisors), and log of prior facility contacts.
  - 3.5.11. Within 30 days of the contract start date, obtain from the prior NHSCR reports of technical assistance between NHSCR and reporters. Maintain these files or modify or upgrade them with approval of the DHHS.
  - 3.5.12. Within 30 days of the contract start date, maintain a computerized log of all abstracts received from each reporting facility that includes facility ID, number of abstracts received, date received, format of data received and NAACCR version if electronic submission.
  - 3.5.13. Within 30 days of the contract start date, obtain from the prior NHSCR vendor copies of hard copy logs and electronic logs of abstracts submitted to NHSCR. Maintain these files or modify or upgrade them with the approval of DHHS. The DHHS will provide necessary contact information and facilitate this transfer.
  - 3.5.14. Upgrade or replace user software and or hardware and make necessary changes to customize software because of advancing technology and or modifications required by DHHS, NPCR or NAACCR standards. Make further upgrade(s) or replacements(s) during the life of this contract, at an additional negotiated price, if so requested by DHHS and subject to all necessary state approvals.
  - 3.5.15. Within 30 days of the contract start date, provide means for DHHS staff approved by the DHHS to periodically receive data from NHSCR, while maintaining data security.
  - 3.5.16. Develop and implement procedures for granting access to data to approved NHSCR staff.
- Q4. *Provide a schematic of the proposed IT set up, including configuration of the hardware (e.g. servers, computers), software, firewalls, and a written description of the configuration. Include a description of the data encryption to be deployed within different components of the IT environment.*



## New Hampshire Department of Health and Human Services Cancer Registry Operations

### 3.6. Database Management Activities

Delete 3.6.4.

Replace with:

- 3.6.4. Assure that the individual case records in the NHSCR automated database are computer-edited for duplicate records, invalid coding, improbable values, and inconsistencies prior to statistical processing and data compilation for analytical purposes. Areas to be edited include, but are not limited to:
- 1 Data Range Checks;
  - 2 Geographic Coding Assignment;
  - 3 Duplicate Record Checks.

### 3.7. Information and System Security Policies and Procedures

Delete 3.7.

Replace with:

### 3.7. Information and System Security Policies and Procedures

- 3.7.1. Maintain the confidentiality and integrity of information in accordance with the Health Insurance Portability and Accountability Act, Public Law 104-191 (<https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996>) and with the Standards for Privacy and Security of Individually Identifiable Health Information, 45 CFR Parts 160 and 164 (<http://www.hipaasurvivalguide.com/hipaa-regulations/hipaa-regulations.php>) and those parts of the HITECH Act as applicable (<http://www.hipaasurvivalguide.com/hitech-act-summary.php>). The contractor shall also maintain and protect the confidentiality of the database and information obtained and maintained during this contract in accordance to NH RSA 141-B (<http://www.gencourt.state.nh.us/rsa/html/X/141-B/141-B-mrg.htm>) and NH Administrative Rules He-P 304 ([http://www.gencourt.state.nh.us/rules/state\\_agencies/he-p300.html](http://www.gencourt.state.nh.us/rules/state_agencies/he-p300.html)) and shall acknowledge agreement with the Data Use Policy of the DHHS, which views NHSCR database as DHHS-owned database, with data release subject to restrictions and conditions.
- 3.7.2. Maintain the security of the system environment in accordance with the requirements of the Cancer Data Registry Technical Requirements in Appendix F, the United States Commerce Department's National Institute of Standards and Technology (NIST) Special Publication 800-53 and the Open Web Application Security Project (OWASP).
- 3.7.3. Maintain a system security and integrity manual which includes plans, procedures and protocols for ensuring that the contractor's NHSCR system will be properly secured, maintained and updated throughout the contract term.
- 3.7.4. Within 14 days after initial contract start date, implement a series of internal procedures to ensure that:
1. Access to automated information is restricted to authorized persons, on a needed basis, and control is maintained over all the documents that contain sensitive information to ensure that these documents are available only to authorized persons.
  2. Implement full security measures to ensure the security and quality of all the elements in the NHSCR database through procedures that shall include the



## New Hampshire Department of Health and Human Services Cancer Registry Operations

---

following:

- i. Ensure that equipment is protected from theft and accidental or deliberate damage or misuse
  - ii. Ensure that once computer programs and data sets are completed and in routine use, they are protected against tampering. Carefully control access to and maintenance of computer programs and NHSCR database.
  - iii. Ensure that copies of original data submitted are maintained and never altered.
  - iv. Ensure that data are protected against inadvertent or deliberate destruction, modification, or dissemination.
  - v. Ensure procedures for backup, archiving, and disaster recovery for computer programs and NHSCR database.
  - vi. Ensure that password are changed, access denied and other security procedures are in place to protect against ongoing access and sabotage when staff resign, are terminated, or no longer assigned to NHSCR contract.
- 3.7.5. Maintain the security and integrity of the NHSCR data. Re-process data at no additional cost to the DHHS in accordance with DHHS instructions if the DHHS or contractor finds that contractor has corrupted, altered, tampered with, or improperly coded/processed any data sets during the duration of the Contract.
- 3.7.6. Immediately report to the DHHS all errors or anomalies in the NHSCR data which could reasonably believe to suggest that security or integrity of the NHSCR or its data may be compromised. The results of any analysis shall be reported to the DHHS and, in addition, the steps it has taken or intends to take to ensure security and integrity of the NHSCR and its data.
- 3.7.7. Implement appropriate policies, procedures and protocols to identify active breaches or threatened breaches of the NHSCR security integrity.
- 3.7.8. Report to DHHS any suspected breach to the NHSCR data in accordance with the requirements in Appendix F, A-7.
- Q7. *Describe your strategy to manage and maintain security and confidentiality of data and of all elements in the database and system. Include plans, procedures, and protocols for ensuring that the contractor's NHSCR system will be properly secured, maintained, and updated throughout the contract term.*

### 3.9. Quality Assurance and Control (QA/DC) Activities

**Delete 3.9.4.**

**Replace with:**

- 3.9.4. By October 31st of each year, obtain from each reporting hospital "diagnostic index" for case finding at all hospital reporting facilities. A diagnostic index is a detailed patient listing of all discharges meeting certain definitions in medical records coding. Encourage facilities to submit electronic diagnostic indices.

**Delete 3.9.6.**

**Replace with:**



## New Hampshire Department of Health and Human Services Cancer Registry Operations

---

- 3.9.6. For each hospital, as resources allow, the key variables specified by NAACCR and NPCR will be selected for visual editing of 25 cases at least every five (5) years for experienced registrars, but up to 100 annually for less experienced registrars or registrars who have not achieved an error rate of <2%. If, after review and discussion with the hospital registrar, the error rate identified in total from these fields is greater than 2%, then the NHSCR will continue to visually edit cases from that hospital and will work with the hospital registrar to improve abstracting.

### 3.10. Reporting Activities

#### Delete 3.10.

#### Replace with:

- 3.10.1. Produce quarterly timeliness and completeness reports by hospital to monitor case reporting activities. Supply aggregate timeliness and completeness reports to DHHS on a quarterly basis, stating which hospitals are delinquent in their reporting and the steps taken to improve reporting from delinquent hospitals.
- 3.10.2. Provide the DHHS with a commentary relating to the annual reports provided by NPCR and NAACCR. Contingent upon receipt of complete death certificate data from New Hampshire Vital Records provide an annual report monitoring completeness estimating the percent of cases with histological verification (HV%) and percent of cases identified by death clearance only (DCO%). Submit a report to DHHS upon completion of the contract period or reasonable amount of time when the NAACCR and NPCR reports are available.
- 3.10.3. Prepare and submit to the DHHS staff a semi-annual review of contract progress by January 15 and August 15 of the contract period. Provide an update of progress on all contract items through the routine semi-annual NHSCR progress report or work plan.
- 3.10.4. Cooperate with any audit of NHSCR for data quality by NPCR or NPCR designated contractor. Submit to DHHS a summary of this audit upon completion.
- 3.10.5. Provide by December 30th of each year of the contract, a finalized data set that has undergone complete QA/QC process. The extract of the data would cover from January 1, 1995 to date.
- 3.10.6. Upon approval from the DHHS, submit finalized datasets to NAACCR and to NPCR as specified by the NAACCR and NPCR standards and Call for Data requirements. Submit copies of each of these submissions to DHHS.
- 3.10.7. Provide cancer case data to and receive data from states with which DHHS has a data exchange agreement, in accordance with the terms of the exchange agreement. The data shall be submitted using the agreed upon NAACCR format and will have been edited to the best extent possible. The DHHS currently has exchange agreements with 7 states and additional agreements may be executed by the DHHS during the life of this contract and shall be accommodated by the contractor.
- 3.10.8. Upon approval of the DHHS, provide selected health researchers, with electronic copies of NHSCR data for certain specific data elements requested and cleared by DHHS.
- 3.10.9. Upon approval from the DHHS, provide data to the Vermont Breast and Cervical Program for breast and cervical cancer cases among Vermont residents diagnosed in New Hampshire in accordance with the program's approved application for data release by DHHS.



## New Hampshire Department of Health and Human Services Cancer Registry Operations

- 3.10.10. Upon approval from the DHHS, provide colorectal cancer case data to the NH Colorectal Cancer Screening Program in accordance with the program's approved application for data release by DHHS.
- 3.10.11. Upon approval from the DHHS, provide breast cancer case data to the NH Mammography Network in accordance with the program's approved application for data release by DHHS; receive cancer case data from the NH Mammography Network.
- 3.10.12. Direct any requests for data or analysis of NHSCR data from researchers, the media or general public to the DHHS within 3 working days of receipt of the request.

### 3.11. Other Programmatic Activity

#### Delete 3.11.5

#### Replace with:

- 3.11.5. Provide Ad-hoc services related to cancer epidemiology. Working with DHHS staff at DHHS offices, the time spent may be up to 12 hours per week on such tasks, as long as suitably qualified staff is available. These tasks will be mutually agreed upon by the contractor and the DHHS, and supervised by the DHHS staff. Tasks associated with these services may include:
  1. Assist in the preparation of data and narrative for the annual cancer report for New Hampshire;
  2. Assist in the investigation of cancer clusters and response to concerns about the occurrence of cancer clusters in New Hampshire;
  3. Assist with the preparation of manuscripts for publication and develop preparatory materials for professional meetings based on the DHHS needs.
  4. Provide Institutional Review Board for the DHHS Chronic Disease Prevention and Screening Section activities.
  5. Enter into agreements with other organizations as needed for processing data according to the NPCR standards, for example, with the National Death Index to obtain death data, and with the Veterans Administration (VA) to obtain VA cancer data.

### 3.12. 3.13. Transition Activities

#### Delete 3.13.1. #3

#### Replace with:

- 3.13.1.
  3. Within 30 days before the end of the contract period, train up to four people employed by the new vendor, by means of a reasonable exchange of information on administration of the NHSCR database, including an overview of reporters and data exchange processes with other states. The training is anticipated to involve at least the vendor's database manager and Quality Assurance supervisor for approximately two days.



## New Hampshire Department of Health and Human Services Cancer Registry Operations

---

### 3.14. Work Plan

Delete 3.14.3.

Replace with:

- 3.14.3. Within fourteen (14) calendar days after the Kick-Off meeting, and within 20 days of the contract effective start date, Contractor shall submit a copy of the finalized Work Plan. This plan should include modifications to the technical proposal, within the Price Limitation of the contract, as requested by the DHHS during the Kick-Off meeting. All activities listed in the Work Plan are subject to approval by the DHHS.

### 4.1. Financial Standards

Delete 4.1.1.1.

Replace with:

- 4.1.1.1. US Department of Health and Human Services, Centers for Disease Control and Prevention, New Hampshire State Cancer Registry Grant to support this project are available from the Catalog of Federal Domestic Assistance (CFDA #) 93.752, Federal Award Identification Number (FAIN) #NU58DP003930.

## 9. Additional Information

Add:

### 9.6. Appendix F – Cancer Data Registry Technical Requirements

Appendix F  
Cancer Data Registry Technical Requirements

REQUIREMENTS	VENDOR RESPONSE	VENDOR COMMENTS
<b>General Requirements Vendor Response Checklist</b>		
<b>Instructions:</b>		
<p><b>Vendor Response Column</b> - Place a "Yes" if the implementation of the Service can fully comply with the requirement described in the row, without special customization. A "Yes" can only be used if the requirement describes your standard service. Otherwise, enter an "No"; A "No" can only be used if the requirement will be met in the future or is not available.</p> <p><b>Comments Column</b> - Vendors can provide a brief explanation. Free form text can be entered into this column. This column can be used to propose alternative approaches to fulfilling the requirement.</p>		
<b>A GENERAL DATA SECURITY AND PRIVACY</b>		
A.1 The Vendor shall be strictly prohibited from releasing or using data or information obtained in its capacity as a collector and processor of the data for any purposes other than those specifically authorized by DHHS. Failure to comply could be a violation of NH laws and rules and may lead to voiding of the Contract.		
A.2 The Vendor shall conduct an annual security assessment, performed by an independent third-party security vendor, to verify that the Vendor's environment containing the projects data is secure. Broader Vendor-wide assessments that include the project's systems are acceptable. The Vendor shall provide certification of assessment to DHHS.		
A.3 As the state's agent, the Vendor must provide certification of compliance with the requirements of the Health Insurance Portability & Accountability Act (HIPAA) and DHHS' standard business associate agreement.		
A.4 As the state's agent, the Vendor must provide certification of compliance with the requirements of the United States Commerce Department's National Institute of Standards and Technology (NIST) and the Open Web Application Security Project (OWASP).		
A.5 In carrying out the duties of this Contract, the Vendor shall be the agent and business associate of DHHS. As such, it is bound by applicable State and federal laws regarding health care information.		
A.6 The Vendor shall provide access to the State with a secure FTP or web site to be used by the State for uploading and downloading files.		
A.7 The Vendor shall notify the State's Project Manager of any security breaches within two (2) hours of the time that the Vendor learns of the occurrence.		

Appendix F  
Cancer Data Registry Technical Requirements

REQUIREMENTS	VENDOR RESPONSE	VENDOR COMMENTS
A.8 The Vendor shall ensure its complete cooperation with the State's Chief Information Officer in the detection of any security vulnerability of the Vendor' hosting infrastructure and/or the application.		
A.9 The Vendor shall be solely liable for costs associated with any breach of State data housed at their location(s) including but not limited to notification and any damages assessed by the courts.		
<b>B APPLICATION SECURITY REQUIREMENTS</b>		
B.1 Verify the identity or authenticate all of the system client applications before allowing use of the system to prevent access to inappropriate or confidential data or services.		
B.2 Verify the identity or authenticate all of the system's human users before allowing them to use its capabilities to prevent access to inappropriate or confidential data or services.		
B.3 Enforce unique user names.		
B.4 Enforce complex non-reusable passwords of ten (10) characters or more that contain at least one upper case, one lower case, one numeric, and one symbol.		
B.5 Passwords should be forced to an Administrator reset after three (3) failed attempts.		
B.6 Encrypt passwords in transmission and at rest within the database.		
B.7 Expire passwords after ninety-days days.		
B.8 Authorize users and client applications to prevent access to inappropriate or confidential data or services.		
B.9 Provide the ability to limit the number of people that can grant or change authorizations		
B.10 Provide the ability to enforce session timeouts during State-defined periods of inactivity.		
B.11 Ensure the application has been tested and hardened to prevent critical application security flaws. (At a minimum, the application shall be tested against all flaws outlined in the Open Web Application Security Project (OWASP) Top Ten ( <a href="http://www.owasp.org/index.php/OWASP_Top_Ten_Project">http://www.owasp.org/index.php/OWASP_Top_Ten_Project</a> ))		
B.12 The application shall not store authentication credentials or Sensitive Data in its code.		
B.13 Audit all attempted accesses that fail or succeed identification, authentication, and authorization requirements		
B.14 The application shall log all activities to a central server to prevent parties to application transactions from denying that they have taken place. The logs must be kept for six (6) months		
B.15 The application must allow a user to explicitly terminate a session. No remnants of the prior session should then remain.		

Appendix F  
Cancer Data Registry Technical Requirements

REQUIREMENTS	VENDOR RESPONSE	VENDOR COMMENTS
B.16 The Application Data shall be protected from unauthorized use when at rest		
B.17 Keep any Sensitive Data or communications private from unauthorized individuals and programs.		
B.18 Subsequent application enhancements or upgrades shall not remove or degrade security requirements		
B.19 Conform to all State and Federal laws and regulations regarding data security		
B.20 Create change management documentation and procedures		
<b>C HOSTING REQUIREMENTS</b>		
C.1 The Vendor shall maintain a secure hosting environment providing all necessary hardware, software, and Internet bandwidth to manage the system and data submitters and the State with permission based logins. <ul style="list-style-type: none"> <li>• Access will be via Internet Explorer Version 7, or as otherwise agreed to by DHHS.</li> </ul>		
C.2 The Vendor will not be responsible for network connection issues, problems or conditions arising from or related to circumstances outside the control of the Vendor, ex: bandwidth, network outages and /or any other conditions arising on the data submitters internal network or, more generally, outside the Vendor's firewall or any issues that are the responsibility of the data submitters Internet Service Provider. .		
C.3 Vendor shall provide a secure Tier 3 or 4 Data Center providing equipment, an on-site 24/7 system operator, managed firewall services, and managed backup Services.		
C.4 The Vendor must monitor the application and all servers.		
C.5 The Vendor shall manage the databases and services on all servers located at the Vendor's facility.		
C.6 The Vendor shall install and update all server patches, updates, and other utilities within 60 days of release from the manufacturer.		
C.7 The Vendor shall monitor System, security, and application logs.		
C.8 The Vendor shall manage the sharing of data resources.		
C.9 The Vendor shall manage daily backups, off-site data storage, and restore operations.		
C.10 The Vendor shall monitor physical hardware.		
C.11 The Vendor shall provide validation that they have adequate disaster recovery procedures in place.		
C.12 The Vendor shall have documented disaster recovery plans that address the recovery of lost State data as well as their own. Systems shall be architected to meet the defined recovery needs.		

Appendix F  
Cancer Data Registry Technical Requirements

REQUIREMENTS	VENDOR RESPONSE	VENDOR COMMENTS
C.13The disaster recovery plan shall identify appropriate methods for procuring additional hardware in the event of a component failure. In most instances, systems shall offer a level of redundancy so the loss of a drive or power supply will not be sufficient to terminate services however, these failed components will have to be replaced.		
C.14The Vendor shall adhere to a defined and documented back-up schedule and procedure.		
C.15Back-up copies of data are made for the purpose of facilitating a restore of the data in the event of data loss or System failure.		
C.16Scheduled backups of all servers must be completed weekly.		
C.17 The minimum acceptable frequency is differential backup daily, and complete backup weekly.		
C.18 Tapes or other back-up media tapes must be securely transferred from the site to another secure location to avoid complete data loss with the loss of a facility.		
C.19 If State data is personally identifiable, data must be encrypted in the operation environment and on back up tapes.		
C.20Data recovery – In the event that recovery back to the last backup is not sufficient to recover State Data, the Vendor shall employ the use of database logs in addition to backup media in the restoration of the database(s) to afford a much closer to real-time recovery. To do this, logs must be moved off the volume containing the database with a frequency to match the business needs.		
<b>D HOSTING REQUIREMENTS – NETWORK ARCHITECTURE</b>		
C.21 The Vendor must operate hosting Services on a network offering adequate performance to meet the business requirements for the State application. For the purpose of this RFP, adequate performance is defined as 99.5% uptime, exclusive of the regularly scheduled maintenance window.		
C.22 The Vendor shall provide network redundancy deemed adequate by the State by assuring redundant connections provided by multiple Internet Vendors, so that a failure of one Internet connection will not interrupt access to the State application.		
C.23 The Vendor' network architecture must include redundancy of routers and switches in the Data Center.		
C.24 Remote access shall be customized to the State's business application. In instances where the State requires access to the application or server -resources not in the DMZ, the Vendor shall provide remote desktop connection to the server through secure protocols such as a Virtual Private Network (VPN).		
<b>E HOSTING REQUIREMENTS - SECURITY</b>		

Appendix F  
Cancer Data Registry Technical Requirements

REQUIREMENTS	VENDOR RESPONSE	VENDOR COMMENTS
C.25 The Vendor shall employ security measures that ensure the State's data is protected.		
C.26 If State data is hosted on multiple servers, data exchanges between and among servers must be encrypted.		
C.27 All servers and devices must have currently-supported and hardened operating systems, the latest anti-viral, anti-hacker, anti-spam, anti-spyware, and anti-malware utilities. The environment, as a whole, shall have aggressive intrusion-detection and firewall protection.		
C.28 All components of the infrastructure shall be reviewed and tested to ensure they protect the State's hardware, software, and its related data assets. Tests shall focus on the technical, administrative, and physical security controls that have been designed into the System architecture in order to provide confidentiality, integrity, and availability.		
C.29 In the development or maintenance of any code, the Vendor shall ensure that the Software is independently verified and validated using a methodology determined appropriate by the State. All software and hardware shall be free of malicious code.		
C.30 The Vendor shall authorize the State to perform scheduled and random security audits, including vulnerability assessments, of the Vendor' hosting infrastructure and/or the application upon request.		
C.31 The Vendor shall provide fire detection and suppression system, physical security of and infrastructure security of the proposed hosting facility. The environmental support equipment of the Vendor website hosting facility: power conditioning; HVAC; UPS; generator must be acceptable to the State.		
<b>F HOSTING REQUIREMENTS - SERVICE LEVEL AGREEMENT</b>		
C.32 The DHHS and Health Facilities shall have unlimited access, via phone or Email, to the Vendor Help Desk technical support staff between the hours of 8:30am to 5:00pm- Monday thru Friday EST.		
C.33 The Vendor telephone or e-mail response time for technical support shall be no more than twenty-four (24) hours.		
C.34 The Vendor shall guarantee 99.5% uptime, exclusive of the regularly scheduled maintenance window		