

Solicitation 042CDMFY10037

Adult Custody Medical Specialty Telemedicine Pilot Project



County of Orange

Bid 042CDMFY10037 Adult Custody Medical Specialty Telemedicine Pilot Project

Bid Number	042CDMFY10037
Bid Title	Adult Custody Medical Specialty Telemedicine Pilot Project
Bid Start Date	May 26, 2010 1:20:26 PM PDT
Bid End Date	Jun 18, 2010 4:00:00 PM PDT
Question & Answer End Date	Jun 14, 2010 4:00:00 PM PDT
Bid Contact	Brian Greene 714-834-3019 bgreene@ochca.com
Contract Duration	1 year
Contract Renewal	Not Applicable
Prices Good for	Not Applicable
Pre-Bid Conference	Jun 4, 2010 1:00:00 PM PDT (Online) Attendance is optional
Standard Disclaimer	The County of Orange is not responsible for and accepts no liability for any technical difficulties or failures that result from conducting business electronically.

Item Response Form

Item	042CDMFY10037-1-01 - Adult Custody Medical Specialty Telemedicine Pilot Project
Quantity	1 year
Unit Price	
Delivery Location	County of Orange <u>183 - HCA/CONTRACT SERVICES</u> 405 W 5TH ST ROOM 600 SANTA ANA CA 92701 Qty 1

Description

As part of its on-going efforts to improve access and provide cost efficient medical care in the Orange County Jails, the County of Orange Health Care Agency (HCA) is seeking proposals from organizations interested and capable of providing specialized medical care, via telemedicine, to adults in the Orange County Sheriff's Department custody. Telemedicine means medical services and/or consultation provided through an electronic video process for inmate/patient care. Telemedicine services through this SIQ are to be provided as a pilot project, designed to evaluate the cost and benefits of these services and shall be for a period of at least one year from the date services begin.



COUNTY OF ORANGE HEALTH CARE AGENCY

FINANCIAL AND ADMINISTRATIVE SERVICES Contract Development and Management



DAVID L. RILEY
DIRECTOR

BOB WILSON
DEPUTY AGENCY DIRECTOR
FINANCIAL AND ADMINISTRATIVE
SERVICES

ALICE MOORE
DIVISION MANAGER
CONTRACT DEVELOPMENT
AND MANAGEMENT

MAILING ADDRESS:
405 W. 5TH STREET, SUITE 600
SANTA ANA, CA 92701

TELEPHONE: (714) 834-5809
FAX: (714) 834-4450

DATE: May 26, 2010

TO: Interested Parties

FROM: County of Orange, Health Care Agency
Contract Development and Management

SUBJECT: **SOLICITATION OF INTEREST AND QUALIFICATIONS (SIQ):
ADULT CUSTODY MEDICAL SPECIALTY TELEMEDICINE PILOT PROJECT**

As part of its on-going efforts to improve access and provide cost efficient medical care in the Orange County Jails, the County of Orange Health Care Agency (HCA) is seeking proposals from organizations interested and capable of providing specialized medical care, via telemedicine, to adults in the Orange County Sheriff's Department custody. Telemedicine means medical services and/or consultation provided through an electronic video process for inmate/patient care. Telemedicine services through this SIQ are to be provided as a **pilot project**, designed to evaluate the cost and benefits of these services and shall be for a period of at least one year from the date services begin. If you are interested in, and capable of, providing the requested services by contract with the County of Orange, please carefully review this SIQ and submit your proposal as directed in the "Proposal Preparation Instructions".

This SIQ is not in any way to be construed as an agreement, obligation, or contract between the County of Orange and any party submitting a proposal to participate in the pilot project, nor will the County pay for any costs associated with the preparation of any proposal.

Bidders submitting proposals must submit the original proposal and three (3) copies. In order to be considered, proposals must be submitted no later than 4:00 p.m. on Friday, June 18, 2010.

In addition, **an electronic copy** of the proposal in PDF format, **is required to be uploaded via BidSync**. Please send hardcopies of your proposal to:

Brian Greene, Contract Administrator
Health Care Agency – Contract Development and Management
405 West Fifth Street, Suite 600, Santa Ana, CA 92701
Phone: 714-834-3019 FAX: 714-834-4450 E-mail: bgreene@ochca.com

All questions regarding this SIQ are to be posted online via the BidSync Question and Answer section. Responses from HCA will be posted as promptly as possible. The Question and Answer section will be closed to new questions on Monday June 14, 2010 at 4:00 P.M. An **online** Bidders' Conference has been scheduled to answer questions you may have regarding the SIQ. Representatives of the Health Care Agency look forward to the opportunity to discuss with you and respond to your questions at that time.

DAY/DATE: Friday June 4, 2010

TIME: 1:00 P.M.

Please log in to the BidSync system at the above date and time to participate in the Bidders' Conference. The Bidders' Conference transcript will also be available via the BidSync website.

If after your review of the SIQ, you do not intend to respond, please feel free to forward it to known interested parties. Your consideration of this solicitation is appreciated.

County of Orange Health Care Agency



SOLICITATION OF INTEREST AND QUALIFICATIONS FOR ADULT CUSTODY MEDICAL SPECIALTY TELEMEDICINE (PILOT PROJECT)

RELEASED

May 26, 2010

SIQ Table Of Contents

SECTION	PAGE
I. Introduction	
A. Background and SIQ Focus	5
B. Eligibility to Submit Proposals	6
C. Funding Availability	7
D. Evaluation of Proposals	7
E. Protest Process	8
F. Confidentiality	8
II. Description of Services	
A. Target Population	9
B. Facilities	9
C. Services	9
1. Telemedicine Services	9
2. Physician Duties	10
D. IT Requirements	11
E. Collaborative Responsibilities of Parties	13
III. Proposal Preparation Instructions	14
IV. Agency Description Information	15
V. Proposal for Telemedicine Services in Custody Setting	
A. Provider Experience/Qualifications	16
B. Staffing	16
C. Proposed Rate	16
D. Timeline	17
E. Equipment and Software	17
VI. Forms	
A. Proposal Preparation Checklist Form A	19
B. Agency Description Form B	20
C. Board of Directors Form C	22
D. Other Funding Sources Form D	23
E. Related Services Experience Form E	24
F. Proposed Rate Form F	25
ATTACHMENT A	
HCA Vendor Security Requirements: Application Service Provider Questionnaire	

INTRODUCTION**SECTION I****A. BACKGROUND AND SIQ FOCUS**

The County of Orange (County), Health Care Agency (HCA) is seeking a telemedicine provider to provide medical services and/or consultation to adult inmates within the Orange County Sheriff Department's (OCSD) correctional facilities. Inmates will attend telemedicine medical specialty clinics at the Central Jail Complex (CJX). It is anticipated that a single contract will be awarded to a provider who can provide all of the required telemedicine services identified in this SIQ under the pilot project.

Orange County's Correctional Medical Services (CMS)

Per California Code of Regulations, Title 15, Article 11 responsibility for correctional health care services rests with OCSD. OCSD ensures the provision of emergency and basic health care services to all inmates through a Memorandum of Understanding (MOU) with HCA. OCSD works collaboratively with HCA to ensure that all regulatory and statutory requirements related to correctional health care are met and that there is adequate space to provide health care services within the correctional facilities.

CMS provides emergency and basic correctional health care services 24 hours per day, seven days per week to meet the immediate medical needs and/or to maintain the health of approximately 4,900 inmates. Health care is provided in keeping with community standards within the program's scope of services. Inmates are provided medical care from the time of their admission, throughout their period of incarceration, and until released. Matters of judgment regarding health care services are the sole responsibility of the CMS health care staff.

Whenever possible, CMS provides medical care on-site in order to most efficiently and effectively meet the inmate's medical needs. Specialized medical services, beyond the scope of on-site services, are referred to off-site contracted providers. These services include specialty consults, treatments, emergency and hospital in-patient level care. Inmates are referred to these contract facilities when deemed appropriate by an on-site CMS medical practitioner.

HCA is interested in offering certain specialized care to inmates through telemedicine, to reduce the number of off-site medical appointments and evaluate telemedicine as a cost saving measure. Specifically, the current identified telemedicine medical specialty services requested through this SIQ are:

1. Oncology;
2. Cardiology;
3. Neurology;
4. Otolaryngology, and
5. Pulmonary.

HCA reserves the right to add or delete medical specialty services based on program need or to terminate this pilot project at any time with advanced notice to provider.

Near the conclusion of the resulting contract period for the pilot project, HCA will evaluate the efficacy of telemedicine in the Orange County jails. Evaluation criteria will include, but not be limited to: cost of services compared to in-house services; cost of services compared to off-site services; and wait times for appointments.

INTRODUCTION**SECTION I**

HCA will work collaboratively with the provider in the evaluation of this telemedicine pilot project and the provider shall submit to HCA, within ninety (90) days prior to the end of the project, a comprehensive report on the telemedicine pilot project, including suggestions and recommendations for improvement.

At the conclusion of the evaluation, HCA may elect to:

- Continue the pilot project for another defined period with the current provider, with or without adjustments to the current telemedicine program, including but not limited to, adding or deleting specialties;
- Release a new solicitation for another pilot project if current provider is unable to provide services requested by HCA;
- Implement a full telemedicine program, with or without adjustments, under an agreement with the current provider or select another provider through a new solicitation, for a period up to three years;
- Terminate the telemedicine program.

B. ELIGIBILITY TO SUBMIT PROPOSALS

This SIQ requests proposals from organizations/individuals that are qualified and interested in contracting to provide the services described within this SIQ in Orange County.

Eligible Applicants

- Organizations that employ or contract with at least one California licensed, board certified specialist trained in telemedicine services, in each of the five specialties listed in Section A., above.
- Organizations with a facility in Orange County that is electronically secure and can be accessed by its physicians to provide telemedicine services at regularly scheduled clinics as established by the County.

To be eligible to submit a proposal, a bidder must **not** be listed on the current Cumulative Sanction List of the Office of the Inspector General (U.S. Department of Health and Human Services) or the General Services Administration's list of parties excluded from federal programs. **HCA will not review a proposal submitted by an individual or entity on either list.**

HCA plans to use the following links to identify individuals and entities that are not eligible to contract with the County of Orange: <http://exclusions.oig.hhs.gov/> & <http://www.epls.gov/>. **Each bidder should verify that it is not on either list prior to preparing a proposal to submit in response to this SIQ.** Correction of any errors found on either sanction list is the sole responsibility of the bidder and must be made prior to the day the proposal is submitted.

HCA requires all potential individuals and/or contract entities to self-disclose any pending charges or convictions for violation of criminal law and/or any sanction or disciplinary action by any federal or state law enforcement, regulatory or licensing agency or licensing body, including exclusion from Medicare and Medicaid programs.

During the term of the Agreement between the contractor and HCA and in accordance with its existing provisions, if a contractor and/or individual become an ineligible persons, the contractor and/or individual shall be removed from any responsibility and/or involvement with HCA contracted obligations related to any direct and/or indirect federal or state health care programs and any other

INTRODUCTION**SECTION I**

federal and state funds. Ineligible Persons is defined as any individual or entity who is currently excluded, suspended, debarred or otherwise ineligible to participate in the federal health care programs; or has been convicted of a criminal offense related to the provision of health care items or services and has not been reinstated in the federal health care programs after a period of exclusion, suspension, debarment, or ineligibility.

C. FUNDING AVAILABILITY

Funding for the contracts resulting from this SIQ is contingent upon sufficient funds being made available by federal, state, and/or county governments for the term of the contract. HCA reserves the right to revise the funding amount and the contract term stated in this SIQ.

D. EVALUATION OF PROPOSALS

An evaluation panel will be established that may consist of representatives of the HCA's CMS staff, and other County staff having knowledge of the services described in this SIQ. The evaluation will consist of a thorough review of the bidders' proposals, and may include interviews with the bidders. Selection of a provider or providers will not be based solely on cost. Cost will be weighed with other factors including, but not limited to; administrative control, program experience, program design, program management, relevant professional expertise, and past performance in delivering contracted services to HCA or other community or governmental entities.

Following a review of proposals by panel members, the HCA Director will approve a recommendation regarding the selection of a service provider. Award of a contract will not be effective until all negotiations have been completed and a final project plan has been agreed upon by all parties as outlined in Section II.E of this SIQ, and/or until authorized by the County of Orange Board of Supervisors, if necessary. The County reserves the right to accept any proposal as offered, to reject any or all proposals, or, based upon the County's needs or availability of funding at the time of selection of a provider or during contract negotiations, to modify the scope of service. The County, at its sole discretion, reserves the right to contract for all or some of the stated services and to cancel this SIQ in whole or in part. Proposals must be valid for a minimum of 120 days from the due date of this SIQ.

The County reserves the sole right to interpret or change any provision of the SIQ at any time prior to the proposal submission date. Such interpretations or changes shall be in the form of a written addendum to this SIQ. Such addendum shall become part of this SIQ and part of any resultant agreement. Such addendum shall be made available to each person or agency that has received an SIQ. Should such addendum require information not previously requested, the County, at its sole discretion, may determine that a time extension is required for the submission of proposals, in which case an addendum will indicate the new proposal submission date.

Activity	Day	Date
SIQ Released	Wednesday	May 26, 2010
Bidders' Conference	Friday	June 4, 2010
Proposals Due	Friday	June 18, 2010
Award Announcement	Friday	July 30, 2010
Services Commence	Wednesday	September 1, 2010

INTRODUCTION**SECTION I****E. PROTEST PROCESS**

In the event a bidder believes that this RFP is unfairly restrictive or ambiguous or contains conflicting provisions, the bidder must submit a written protest to the HCA Contract Development and Management Division Manager no later than five (5) business days prior to the proposal deadline. Protests of specifications and/or solicitation terms and conditions made after the five (5) business day deadline will not be considered by the County. In the event the protest of specifications is denied and the protestor wishes to continue in the solicitation process, they must still submit a proposal prior to the proposal deadline, in accordance with the RFP submittal procedures.

Protests of award of contract must be submitted to the HCA Contract Development and Management Division Manager no later than five (5) business days after the notice of the proposed contract award is given by the HCA Director. Protests relating to a proposed contract award which are received after the five (5) business day deadline will not be considered by the County. All protests must include the following information:

1. The name, address, and telephone number of the protester;
2. The signatures of the protestor or the protester's authorized representative;
3. The name/requested services of the RFP;
4. A detailed statement of the legal and/or factual grounds of the protest; and
5. The form of relief requested.

Written protests must be sent to:

County of Orange/Health Care Agency
Contract Development and Management
405 West Fifth Street, Sixth Floor
Santa Ana, CA 92701-4637

F. CONFIDENTIALITY

Pursuant to California law, all information contained in your response to this RFP may be public record subject to disclosure to any member of the public who requests it. If it is necessary to include proprietary/trade secret information in your response, the County recommends that you clearly and prominently mark the information that you believe falls within this category. The County will attempt to notify you if disclosure is requested of information that you have indicated is proprietary/trade secret information, in order to give you an opportunity to seek a court order prohibiting disclosure of such information. However, due to the short statutory time period of the County's responses to request for public records, the County will be able to give you only a short period of time in which to seek such a court order before the County will be required to disclose the requested information. Further, it is entirely your responsibility to assert that information you believe is proprietary/trade secret information should not be disclosed; the County will not make such a claim for you, but will obey a valid court order obtained by you prohibiting disclosure of such information.

DESCRIPTION OF SERVICES**SECTION II****A. TARGET POPULATION**

Orange County jail inmates can be minimum to maximum security risk. The current average daily population system-wide is approximately 4,900 inmates, with 87% male and 13% female. Approximately 4% of the population is 56 years or older, 20% 41 to 55 years, 23% 31 to 40 years, 22% 25 to 30 years, 12% 22 to 24 years, and 19% is 18 to 21 years old. Ethnicity is approximately 51% Hispanic, 35% Caucasian, 7% African American, 3% Vietnamese, and 4% other. Approximately 70% are in custody on felony charges and 30% on misdemeanor charges, with 60% pre-trial and 40% sentenced. The average length of stay for pre-trial inmates is 214 days and 86 days for sentenced inmates.

Inmates are provided with appropriate medical care to address their injuries and/or illnesses. For this pilot project approximately six (6) scheduled inmate/patient visits are currently estimated for each monthly telemedicine specialty clinic identified in this SIQ, for a combined estimated total of sixty (60) clinics with three hundred sixty (360) scheduled inmate/patient appointments in a one year period.

B. FACILITIES:

The CJX is located next to the Sheriff's Headquarters building in Santa Ana. Approximately 2,664 inmates are housed at the CJX which includes the Men's Jail, the Intake and Release Center, and the Women's Jail (temporarily closed since July 2009). OCSD also operates the Theo Lacy and James Musick Facilities. Medical, dental, and mental health evaluation and treatment areas are designated within each facility.

Inmates from all facilities, with OCSD approval, will be escorted to a single location, suitable for inmate/patient exams and consults within the CJX facility for all telemedicine clinics. When not in use, the telemedicine equipment will be stored in a secure locked location.

C. SERVICES

The selected provider shall be able to provide telemedicine medical specialty services from a remote location in Orange County to adult inmates during clinics held in the OCSD CJX. The provider will coordinate with the CMS medical and administrative managers to ensure effective and cost efficient services during the pilot project. In addition, the provider will furnish all personnel, electronic equipment and software, materials, facilities, and any other services necessary to accomplish delivery of the following services.

Telemedicine Services:

California licensed, board certified physicians in Oncology, Neurology, Cardiology, Otolaryngology, and Pulmonary will provide specialized medical care to adult inmates in the Orange County jails, via telemedicine. Trained physicians at a remote electronically secure facility/location will be available for "real-time" communication with the inmates/patients and medical staff at CJX.

Telemedicine clinics will be held once a month for each specialty. Each specialty clinic is anticipated to be approximately two hours in duration, with an anticipated volume of six (6) inmate/patients per clinic. The clinic schedules and hours shall be coordinated with CMS and OCSD.

DESCRIPTION OF SERVICES**SECTION II**

HCA may revise medical specialty services provided during this pilot project, based on program need.

The provider selected for the pilot project shall:

1. Provide and maintain all necessary electronic videoconferencing and diagnostic telemedicine equipment and related software to be used in CJX and at the provider's electronically secure facility to diagnose and treat inmates/patients at medical specialty telemedicine clinics.

Equipment and connectivity must meet HCA's specifications, and provider must meet IT security requirements, as outlined in the "IT Requirements" listed below. All Bidders must complete the County of Orange Health Care Agency Vendor Security Requirements package (attachment A) in order to have a responsive bid.

2. Recruit, screen, train, manage, and compensate California licensed, board certified physicians capable of providing the medical services described in this SIQ.
3. Ensure physician availability for all scheduled clinics, unless clinic is cancelled by CMS with at least 24 hour notice.
4. Provide training for CMS medical staff assigned to telemedicine clinics on the use of the videoconferencing and diagnostic equipment. **NOTE: All employees and/or subcontractors that will enter the CJX facility will be required to pass a security clearance prior to admission. This clearance will be valid for a period of one year from the date issued.**
5. Designate staff to coordinate clinic appointments with CMS, and to receive and forward all communication between provider's physicians, CMS and contract physicians.
6. Provide all reports required by HCA/CMS, including monthly reports related to clinic schedules and services identifying kept and missed appointments, additional recommended treatment, and inmate/patient utilization trends.
7. Provide copies of inmate/patient health records or information therein as requested by HCA, and in keeping with HIPAA and other applicable privacy laws and regulations.
8. Designate liaison to meet with CMS Medical Director and the Director of Nursing regularly on quality assurance, utilization review and other issues affecting the service delivery system.
9. Maintain medical record information on each inmate/patient seen via telemedicine, in compliance with all patient confidentiality laws and regulations for a minimum of seven (7) years, either at provider's location or at another location as approved in advance by HCA.

Physician Duties:

The provider's California licensed, board certified physicians shall be trained in the use of telemedicine equipment and shall:

1. Assess and monitor inmate/patient medical conditions during scheduled telemedicine clinics using appropriate electronic diagnostic equipment, and determine appropriate course of medical treatment. CMS medical staff (Medical Assistant or Nurse) at CJX will assist the physician during inmate/patient visit.

DESCRIPTION OF SERVICES**SECTION II**

2. Provide legible written summary for each inmate/patient telemedicine visit/consult within five days including, at a minimum, patient complaint, diagnosis, physician assessment and treatment recommendations, patient condition and recommended follow-up. Information shall be provided to CMS via fax, mail or encrypted e-mail and shall be sufficient to support continuity of care.
3. Be available by telephone or videoconferencing to consult with CMS jail physicians, contracted medical specialists, and contract hospital staff during normal work hours (approximately 7 a.m. to 6 p.m.) to ensure quality medical care and continuity of care for inmates/patients.
4. Adhere to all inmate/patient confidentiality and HIPAA requirements.

All services must be provided in accordance with all applicable State of California laws and regulations governing medical services.

D. IT REQUIREMENTS

HCA must maintain the security of its information and information processing facilities in all instances, including when those assets are accessed, processed, communicated to, managed, transacted, or stored by external parties. The security of the County's information and information technology infrastructure must not be compromised by the introduction of third party products or services, whether during normal operations or in the event of a business disruption. Accordingly, access to HCA's information and assets must be controlled at all times.

HCA requires that all providers, whose product falls within the realm of information technology which is housed at HCA, meet a minimum set of functional and technical security requirements and comply with the County's security policy and HCA's security standards. This shall include, but not be limited to, the following:

System Guidelines & Requirements:

1. Vulnerability management
2. Server and workstation hardening
3. Business continuity planning
4. Change management
5. System monitoring and logging
6. Physical and environmental security
7. Information security incident management

Application Functionality:

1. Encryption:
 - a. Application is required to use encryption to protect sensitive data in both storage and during transmission wherever technically possible.
 - b. All encryption methods must defined by the provider.
2. Access Management:
 - a. Application will support role-based functionality (user authenticated and assigned a role, with access controlled based on that role).
 - b. Application will support measures to define, attach, modify and remove access rights for all classes of users.
 - c. Application will support measures to enable and restrict access to the whole and/or sections of the technology solution in accordance with prevailing consent and access rules.

DESCRIPTION OF SERVICES**SECTION II**

- d. Successful bidder will work toward meeting the evolving standards for authentication as they become available.
3. Password Management:
 - a. Application will support password management measures including but not limited to password expiration, account lockout and complex passwords.
 - b. Application will support session inactivity timeouts.
4. Audit Capabilities:
 - a. Application will support the identification of the nature of each access and/or modification through the use of logging.
 - b. Application will employ audit capabilities to sufficiently track details that can establish accountability for each step or task taken in the clinical or operational processes.
 - c. All audit logs will be protected from unauthorized alteration.

Support Functionality:

1. Remote Support:

Application or Successful bidder will be able to audit remote support activities to an individual employee.
2. Configuration Management and Change Control:
 - a. Successful bidder will provide updates to address any applicable security vulnerabilities.
 - b. Successful bidder will define who is responsible for updates to the application and any related operating systems.

Provider Information:

1. Service Level Agreement (SLA):

Successful bidder will define guaranteed response times related to a SLA.
2. Third Party Application Testing:

Successful bidder is required to have independent security testing on their application on, at least, an annual basis and address any found vulnerabilities within a reasonable amount of time.

The successful bidder will be required to submit the following information **during negotiations**, as detailed in paragraph E., below:

Application Functionality:

1. Encryption:

All encryption methods must defined by the provider.
2. Network Communication:

Successful bidder will provide information related to standards and requirements for the deployment of the application, including methods of secure implementation and port requirements.

DESCRIPTION OF SERVICES**SECTION II****Support Functionality:**

1. Remote Support:
Successful bidder will identify the requirements for remote support including all available options.
2. Protection from Malicious Code:
Successful bidder will reveal potential compatibility issues with Commercial off the Shelf (COTS) virus scanning software.

E. COLLABORATIVE RESPONSIBILITIES OF PARTIES

Prior to the execution of an agreement for the implementation of telemedicine services under this SIQ, the proposed winning bidder and HCA, OCSD, staff shall meet and develop a detailed timeline for implementation of the telemedicine clinics that will include the following;

1. Review and approval of bidder's equipment and software by HCA IT staff.
2. Review of all IT standards required by HCA and OCSD and agreed upon compliance of such by the bidder.
3. Review of IT requirements for bidder to implement the telemedicine connections between the CJX and their remote secure location, including items such as ports, internet access connections, bandwidth requirements, security, firewalls, etc.
4. Review of HCA and OCSD requirements for bidder's staff, subcontractor's security screening requirements.
5. Walk through of the CJX facility with bidder to identify location of clinics and storage of bidder's equipment.
6. Walk through of the bidder's secure location and approvals from HCA IT staff.
7. Delivery and installation of equipment to the CJX
8. Testing of telemedicine system between CJX and the remote secure location.
9. Training for CMS staff of the equipment located within the CJX facility.
10. Start Date of Telemedicine Services
11. Schedule for specialty clinics for first 90 days of the pilot project.

In addition to the above timeline, the Parties shall develop and agree upon a coordinated telemedicine service delivery plan that will outline the roles and responsibilities of each party to ensure successful implementation and delivery of telemedicine services during the pilot project.

PROPOSAL PREPARATION INSTRUCTIONS**SECTION III**

Your proposal must clearly meet all of the requirements of this SIQ. Review all requirements and instructions to ensure that each is clearly addressed in your proposal. Prepare the proposal with the reviewer in mind. Proposals should be carefully proofread and include the following:

- ❖ A table of contents (with page numbers);
- ❖ Reference(s) to any appendices;
- ❖ Placement of required forms immediately after the text that relates to them;
- ❖ Numbered pages;
- ❖ Single-sided text that is at least one and one-half (1½) line-spaced; and
- ❖ All of the requested information in the sequence and format specified in the SIQ.

A proposal may be rejected if it is conditional, incomplete, or deviates from the specifications in this SIQ. HCA reserves the right to waive, at its sole discretion, any procedural irregularity, immaterial defect, or other impropriety deemed reasonably correctable or not warranting rejection of the proposal.

1. Use the Proposal Preparation Checklist Form **(Form A)** to plan and monitor proposal preparation, as well as to verify completion of all materials before submission.
2. Follow instructions about the order for presenting information, narrative text, and information requested on the forms.
3. Insert forms immediately after the narrative they support in your proposal.
4. The original and all required copies of the proposal must each be arranged in three-ring binders or spiral-bound notebooks. Loose copies will not be accepted. In addition, **an electronic copy** of the proposal in PDF format, **is required to be uploaded via BidSync.**
5. Within each three-ring binder or spiral-bound notebook, index the original proposal and all copies, with tabs.
6. Provide accurate and honest information. Reviewers tend to respond more favorably to a candid account of problems and creative plans to address them than a glossing over of an apparently problematic situation. Information that is deliberately inaccurate may prompt an investigative review and will affect the evaluation of the proposal.
7. Make sure information provided on the forms is consistent with the narrative and with information provided on other forms.
8. If you omit any required information or data, explain why.
9. Do not assume that reviewers know your program. Your proposal must be completely self-explanatory.
10. Provide documentation where necessary including items such as forms, etc.
11. Do not use appendices for information that is required in the body of the proposal. Use appendices to provide documentation or examples of activities mentioned in the proposal.
12. **Information requested in Section IV is to be provided in one three-ring binder or spiral-bound notebook. Only one copy is required. Information requested in Section V is to be provided in a separate three-ring binder or spiral-bound notebook. Provide an original and three copies of all information requested in Section V, including attached forms and appendices, if any.**

AGENCY DESCRIPTION INFORMATION**SECTION IV**

Submit the following information in one three-ring binder or spiral-bound notebook.

- A. Complete the Agency Description Form **(Form B)**.
- B. Complete the Board of Directors Form **(Form C)**.
- C. Complete the Other Funding Sources Form **(Form D)**.
- D. Provide copies of the following documentation (include an index of all documents included and explanations for any documents requested but not provided):
 - 1. If incorporated:
 - a. Articles of Incorporation, executed by the Secretary of state, **including all amendments**.
 - b. By-laws, including all amendments.
 - c. Board of Directors resolution empowering a Corporate Officer to act on behalf of the organization by his/her signature alone.
 - 2. If not incorporated - Documentation identifying the Authorized Representative who may act on behalf of the organization by his/her signature alone.
 - 3. If doing business under another name - Fictitious Business Name statement filed with the County Clerk, and Proof of Publication.
 - 4. Any partnership papers and/or joint venture agreements.
 - 5. If appropriate – certification of nonprofit status from the State of California **and** the federal government.
 - 6. If appropriate – licenses/certifications and/or Conditional Use Permit (CUP).
 - 7. If appropriate – letter(s) of Probation approval.
 - 8. Recent financial statement, preferably prepared by a Certified Public Accounting firm.
 - 9. Any audits, reviews, or inspection reports completed within the last twelve (12) months.
 - 10. Corporate organizational chart **including all programs** which identifies the relationship of the proposed program to the overall organization **and** which identifies the reporting relationship of each proposed staff position.
- E. Describe any pending audits, pending litigation, and/or investigation involving the organization.

ADULT CUSTODY TELEMEDICINE PILOT PROJECT**SECTION V**

Provide the following information in a second three-ring binder or spiral-bound notebook. Provide an original and three (3) copies of this binder or notebook.

A. PROVIDER EXPERIENCE/QUALIFICATIONS

1. Complete the Related Service Experience Form (Form E) to describe past and current experience in providing services similar to those described in this SIQ. Specify the types of services or projects the organization currently provides, and the length of time the organization has provided each service or project.
2. Discuss your organization's experience and demonstrated ability (including past and present involvement) in providing the services being bid upon in this SIQ, including (**limit your response to four pages of text**):
 - a. Experience and ability to provide medical diagnosis, consultation, monitoring via telemedicine to persons in custody, including those who do not speak English.
 - b. Experience recruiting California licensed, board certified physicians capable of providing telemedicine services in the specialties identified in this SIQ.
 - c. Ability to provide a fully equipped, centralized, electronically secure facility in Orange County, in which physicians can conduct telemedicine clinics, and to provide appropriate telemedicine equipment to be used in the jail.
3. Discuss your organization's experience with the target population identified in Section II.A.

B. STAFFING

1. Identify the staff who will be providing the services described in this SIQ. Include the following:
 - a. Resumes/CV
 - b. Proof of licensure
 - c. Job descriptions
2. If your organization intends to hire staff to provide these services, identify the minimum qualifications for each position.
3. Identify the administrative staff that will have primary responsibility for coordinating the program, including scheduling of clinics.
4. Describe any services that will be subcontracted. Subcontracts must be approved in advance in writing by HCA and must meet the requirements of this SIQ.

C. PROPOSED RATE

Complete the Proposed Rate Form (**Form F**) for each specialty service.

Please note that all payments received from the County for charges incurred under the resulting agreement shall be the total compensation for all services rendered, and the selected provider shall not seek any additional reimbursement.

ADULT CUSTODY TELEMEDICINE PILOT PROJECT**SECTION V**

D. TIMELINE

Provide a timeline that identifies the key tasks to be accomplished in order to begin providing services within 4 weeks of contract execution (hiring any additional staff, etc.). If you will be unable to provide services, provide your proposed schedule for the anticipated start date for services.

E. EQUIPMENT AND SOFTWARE

1. Please provide a detailed list of proposed equipment and requirements that will be used/needed to provide the services required in this SIQ.
 - a. Equipment at providers' secured location;
 - b. Equipment to be placed within the CJX facility;
 - c. Required/Requested hardware / access from County at the CJX facility;
 - d. Software used to provide the services; and
 - e. Other relevant items necessary to provide services.
2. Please provide a completed Application Service Provider Questionnaire (Attachment A).

FORMS

SECTION VI

FORMS

PROPOSAL PREPARATION CHECKLIST**FORM A**

Use this checklist to identify whether or not all items requested have been included. This form is to be completed and included in the proposal, and must be located with the proposal's Table of Contents.

	Item(s) Enclosed/Completed	Page and Section Number
Binder I – Agency Description		
1. Agency Description Form B	_____	_____
2. Board of Directors Form C	_____	_____
3. Other Funding Sources Form D	_____	_____
4. Documentation	_____	_____
a. Articles of Incorporation	_____	_____
b. By-Laws	_____	_____
c. Resolution Empowering Corporate Officer	_____	_____
d. Documentation Identifying Representative	_____	_____
e. Fictitious Business Name and Proof	_____	_____
f. Partnership Papers/Joint Venture Agreements	_____	_____
g. Non-profit Status Certificates	_____	_____
h. Licenses and Permits	_____	_____
i. Financial statements	_____	_____
j. Audits/Reviews/Inspection Reports	_____	_____
k. Corporate Organizational Chart	_____	_____
5. Pending audits/litigations/investigations	_____	_____

PROPOSAL PREPARATION CHECKLIST**FORM A**

	Item(s) Enclosed/Completed	Page and Section Number
Binder II – Programmatic Proposal		
A. Provider Experience/Qualifications		
1. Related Service Experience (Form E)	_____	_____
2. Ability to Provide Proposed Services	_____	_____
3. Experience with target population(s)	_____	_____
B. Proposed Staffing		
1. Identification of Program Staff	_____	_____
2. Identification of Administrative Staff	_____	_____
3. Subcontracted Services	_____	_____
C. Proposed Rate		
1. Proposed Rate (Form F)	_____	_____
D. Timeline		

E. Equipment and Software		
1. Equipment at provider's location	_____	_____
2. Equipment at CJX facility	_____	_____
3. Required/Requested Hardware/Access	_____	_____
4. Software to be used	_____	_____
5. Other relevant items	_____	_____
6. Application Service Provider Questionnaire	_____	_____

AGENCY DESCRIPTION FORM**FORM B**

1. BIDDER'S LEGAL NAME: _____
 (As Specified In The Articles Of Incorporation Or State License)
 BUSINESS ADDRESS: _____

2. **CONTRACT SIGNATURE AUTHORITY** - IDENTIFY BELOW THE PERSON EMPOWERED TO SIGN A CONTRACT:

CORPORATE OFFICER OR AUTHORIZED REPRESENTATIVE NAME: _____

CORPORATE OFFICER OR AUTHORIZED REPRESENTATIVE TITLE: _____

CORPORATE OFFICER OR AUTHORIZED REPRESENTATIVE PHONE #: _____ FAX #: _____

EMAIL: _____

If incorporated - Attach Board of Directors resolution empowering the Corporate Officer identified above to act on behalf of the organization by his/her signature alone.

If unincorporated - Attach documentation identifying the person listed above as an Authorized Representative who may act on behalf of the organization by his/her signature alone.

3. DATE ORGANIZATION ESTABLISHED: _____

4. TYPE OF BUSINESS (CHECK ONE):

☐ Nonprofit Corporation

☐ Other (Specify): _____

5. *IN THE FOLLOWING SECTION, DO NOT INCLUDE ANTICIPATED FUNDS THAT MAY BE AWARDED FROM THIS SIQ:*

ESTIMATED ANNUAL OPERATING BUDGET: \$ _____ for 7/1/09 - 6/30/10

Operating Budget Generated From:

Government Contracts:	\$ _____	_____ %
Non-Governmental Agencies:	\$ _____	_____ %
Donations:	\$ _____	_____ %
Participant Fees:	\$ _____	_____ %
Other (Specify): _____	\$ _____	_____ %
Other (Specify): _____	\$ _____	_____ %
TOTAL:	\$ _____	_____ %

6. **PROPOSAL CONTACT PERSON** - IDENTIFY BELOW THE PERSON WHO WILL REPRESENT THE ORGANIZATION DURING THE PROPOSAL EVALUATION PROCESS:

PROPOSAL CONTACT PERSON NAME: _____

PROPOSAL CONTACT PERSON TITLE: _____

PROPOSAL CONTACT PERSON PHONE #: _____ FAX #: _____

PROPOSAL CONTACT PERSON E-MAIL ADDRESS: _____

PROPOSAL SUBMITTAL AUTHORITY:

The undersigned hereby acknowledges that I have read and understand the contents of, and have authority to submit, the attached proposal on behalf of the above-named organization. It is correct to the best of my knowledge and represents the organization's proposal for the provision of the requested services.

CORPORATE OFFICER OR AUTHORIZED REPRESENTATIVE

DATE

PHONE #

BOARD OF DIRECTORS FORM**FORM C**

Please provide the following information about your Board of Directors.

Number of Members: _____ Term Length: _____ Meeting Dates: _____

Current Office: _____	Membership Commenced: _____
Name: _____	Membership Expires: _____
Address: _____	Board Term Commenced: _____
City/Zip: _____	Board Term Expires: _____
Telephone: _____	FAX: _____
Occupation: _____	Subcommittees: _____
	Other Affiliations: _____

Current Office: _____	Membership Commenced: _____
Name: _____	Membership Expires: _____
Address: _____	Board Term Commenced: _____
City/Zip: _____	Board Term Expires: _____
Telephone: _____	FAX: _____
Occupation: _____	Subcommittees: _____
	Other Affiliations: _____

Current Office: _____	Membership Commenced: _____
Name: _____	Membership Expires: _____
Address: _____	Board Term Commenced: _____
City/Zip: _____	Board Term Expires: _____
Telephone: _____	FAX: _____
Occupation: _____	Subcommittees: _____
	Other Affiliations: _____

Current Office: _____	Membership Commenced: _____
Name: _____	Membership Expires: _____
Address: _____	Board Term Commenced: _____
City/Zip: _____	Board Term Expires: _____
Telephone: _____	FAX: _____
Occupation: _____	Subcommittees: _____
	Other Affiliations: _____

Use additional copies of this page if needed.

OTHER FUNIDNG SOURCES

FORM D

County of Orange Contracts:

☐ Not Applicable

AGENCY/DEPT	FUNDING SOURCE	FUNDING PERIOD	GROSS PROGRAM COST	MEDI-CAL REVENUE	OTHER REVENUE	NET PROGRAM COST
Contact Person Name/Title/Telephone Number:						
Contact Person Name/Title/Telephone Number:						
Contact Person Name/Title/Telephone Number:						

Funding Other Than Through The County of Orange:

☐ Not Applicable

AGENCY/DEPT	FUNDING SOURCE	FUNDING PERIOD	GROSS PROGRAM COST	MEDI-CAL REVENUE	OTHER REVENUE	NET PROGRAM COST
Contact Person Name/Title/Telephone Number:						
Contact Person Name/Title/Telephone Number:						
Contact Person Name/Title/Telephone Number:						
Contact Person Name/Title/Telephone Number:						

Use Additional Copies Of This Page If Needed

RELATED SERVICES EXPERIENCE FORM

FORM E

Identify past and current experience in providing services similar to those requested in this SIQ.

Description of Related Services	Length of Time in Business		Selected Region, City, or Unincorporated Area	Amount of Funding	Funding Source(s)
	Started	Ended*			
1.					
Contact Person/Title/Telephone:					
2.					
Contact Person/Title/Telephone:					
3.					
Contact Person/Title/Telephone:					
4.					
Contact Person/Title/Telephone:					
5.					
Contact Person/Title/Telephone:					

* Enter "Present" if still providing the identified services.

Use additional copies of this page if needed.

PROPOSED RATE FORM**FORM F****Proposed Fee Schedule****Proposer** _____

*Clinic Fees	Cardiology	Neurology	Otolaryngology	Oncology	Pulmonary
Physician					
**Administrative					

Clinic Total \$					
------------------------	--	--	--	--	--

Annual Total \$: 12 Clinics					
--	--	--	--	--	--

Total Proposed Project Fees:	\$				
-------------------------------------	----	--	--	--	--

Bidder's Comments/ explanations:

*Clinics will be held once a month for each specialty and be two hours long.

**Please attach a detailed budget of your proposed Administrative fees including:

Staff Salaries and Benefits prorated to the project

Equipment

Services and Supplies

Profit

Other (describe)

ATTACHMENT A



County of Orange Health Care Agency Vendor Security Requirements

Application Service Provider Questionnaire

05/2010

Table of Contents

1.0 - Overview	3
2.0 - Vendor Instructions	3
2.1 - Example	3
3.0 - Questionnaire	4
3.1 - Vendor Contact Information.....	4
3.2.1 - Encryption	5
3.2.3 - Access Management.....	9
3.2.4 - Password/User Management	10
3.2.5 - Audit Capabilities	13
3.2.6 - Other Capabilities.....	16
3.3 - Support Functionality	17
3.3.1 - Security of Remote Support.....	17
3.3.2 - Protection from Malicious Code	19
3.3.3 - Configuration Mgmt & Change Control.....	20
3.4.1 - Service Level Agreements.....	22
3.4.2 - Third Party Application Testing	22
3.4.3 - Other.....	23
4.0 – Appendix	24



1.0 - Overview

The County of Orange Health Care Agency (OCHCA) requires that all vendors whose product falls within the realm of information technology meet a minimum set of functional and technical security requirements. As such, the Information Security Department has prepared a questionnaire that will help the IT staff more thoroughly understand the security ramifications related to the potential implementation of a vendor's product.

As part of the vendor approval process, the vendor must demonstrate compliance with the OCHCA's Vendor Security Requirements by responding in writing to the statements or questions listed in section three unless otherwise specified within the question. By responding to those statements or questions below, the Information Security department will be able to expedite the security approval process. Failure to respond to all statements and questions may result in your disqualification.

2.0 - Vendor Instructions

The OCHCA Information Security Department is looking for detailed, technical responses to the following statements and/or questions. The vendors should include any supporting documents including but not limited to security whitepapers, technical documents, security policies and/or procedures that you may have that will assist us in understanding your information security profile.

2.1 - Example

Insufficient Response: "Our product uses encryption."

Acceptable Response: "All communications between the clients and server are protected by through 128-Bit SSL encryption on TCP port 7443."

Each applicable section will include a reference section. If the question or statement relates to information referenced within your supporting documents, please provide the document name and page number within the associated reference section.



3.0 - Questionnaire

3.1 - Vendor Contact Information

Application Name:		Version:	Release Date:
Application Supports the following business functions:			
Vendor Representative Contact Information	Name:	Title:	Department:
	Company Name:	Telephone Number:	E-mail:
	Support Number:	Support E-mail:	Website URL:
Contracting Agency/ Department Contact Information	Department:		Telephone:
	Agency Contact:		E-Mail:
Additional Information:			



3.2 - Application Functionality

- 1) Briefly describe your application's function and indicate how the software functions (i.e. Client/Server, Web Based, etc.)

Reference Information

3.2.1 - Encryption

- 2) Does this application employ data encryption?
If no, continue to question 7.
If yes, describe whether it is network-based encryption, storage-based encryption, or both.

☒ Yes

☐ N/A

☐ No

Reference Information

- 3) Does the application encrypt data before sending it over the Internet or an open network?
If yes, indicate the type of encryption.

☒ Yes

☐ N/A

☐ No

Reference Information



Application Service Provider
Questionnaire

Page 5

- 4) Does the application encrypt data before storing on removable media such as backup tapes, CDs, DVDs, etc, or devices such as laptops, tablets, or computer workstation hard disk drives?
If yes, indicate the encryption used.

☒ Yes☐ No☐ N/A

Reference Information

- 5) Is password transmission and storage encrypted and un-viewable even to the system administrators?
If yes, indicate the encryption used.

☒ Yes☐ No☐ N/A

Reference Information



6) Is this application web-based or does this application include a web interface? If no, continue to question 11. If yes, include the types of secure connections that are supported.	☒ Yes ☐ No	☒ N/A ☐
--	--	---

7) Is this application's web interface appropriate to deploy as Internet-facing? If no, please explain.		☒ Yes	☒ N/A
		☐ No	
Reference Information			

8) Are there security safeguards are inherent in the application to protect against network vulnerabilities such as, but not limited to, SQL Injection, Cross Site Scripting, Website Defacement or Hijacking, installation of Trojan horses/spyware, etc.? If yes, please explain.	☒ Yes ☐ N/A ☐ No
Reference Information	



9) If this application is behind our perimeter firewall, are there protocols and IP ports need to be opened? If yes, please explain.	☒ Yes ☐ No	☐ N/A
Reference Information		

10) Should this application be protected by an application proxy? If so, please explain in detail.	☒ Yes ☐ No	☐ N/A
Reference Information		

11) Does this application/system have a typical network setup? Please include information like which network services would be required (i.e. DNS, SMTP, etc.)	☒ Yes ☐ No	☐ N/A
Reference Information		



3.2.3 - Access Management

12) Is the user authenticated to the application? If yes, briefly describe how the user is authenticated to the system. If no or not applicable, please continue to 25.	☒ Yes ☐ No	☐ N/A
Reference Information		

13) Does the application support integration with enterprise identity management systems? If yes, indicate the compatible systems (such as Directory Services, LDAP, Kerberos, etc.)	☒ Yes ☐ No	☐ N/A
Reference Information		

14) Is the application compatible with alternative authentication mechanisms (e.g. certificates, token, biometric, etc.?)	☒ Yes ☐ No	☐ N/A
Reference Information		



3.2.4 - Password/User Management

17) Can the user change their password at any time?	☒ Yes	☐ N/A
	☐ No	



18) Can the system administrator enforce password policy and/or complexity such as minimum length, numbers and alphabet requirements, and upper and lower case letters, etc.?

☒ Yes☐ N/A☐ No

Reference Information

19) Can the application force password expiration and prevent users from reusing a password?

☒ Yes☐ N/A☐ No

Reference Information

20) Can the application be set to automatically lock a user's account after a predetermined number of consecutive unsuccessful logon attempts?

☒ Yes☐ N/A☐ No

Reference Information



Application Service Provider
Questionnaire

Page 11

21) Does the application prohibit users from logging into the application on more than one workstation at the same time with the same user ID?

☒ Yes

☐ N/A

☐ No

Reference Information

22) Can the application be set to automatically log a user off the application after a predefined period of inactivity?

☒ Yes

☐ N/A

☐ No

Reference Information

23) Can the application support the removal of user's access privileges without requiring the deletion of the user account?

☒ Yes

☐ N/A

☐ No

Reference Information



Application Service Provider
Questionnaire

Page 12

3.2.5 - Audit Capabilities

26) Does this application capture user access activity such as successful logon, logoff, and unsuccessfully logon attempts? If yes, list the data elements contained in the audit log.	☒ Yes ☐ No	☐ N/A
---	--	---------------------------

Reference Information



27) Does this application capture data entries, changes, and deletions?
If yes, list the data elements contained in the audit log.

☒ Yes☐ N/A☐ No

Reference Information

28) Does the application time stamp for audit log entries synchronize with other applications and systems using NTP/SNTP?

☒ Yes☐ N/A☐ No

Reference Information

29) Can the audit log "data" be exported from the application for further processing (e.g. storage, analysis)?

☒ Yes☐ N/A☐ No

Reference Information



30) Are the audit log files protected from unauthorized alteration?
If yes, please describe the protections.

☒ Yes☐ N/A☐ No

Reference Information

31) Does the application allow a system administrator to set the inclusion or exclusion of audited events based on organizational policy and operating requirements or limits?

☒ Yes☐ N/A☐ No

Reference Information

32) Can the application continue normal operation even when the security audit capability is non-functional? (For example, if the audit log reaches capacity, the application should continue to operate and should suspend logging, start a new log, or begin overwriting the existing log)

☒ Yes☐ N/A☐ No

Reference Information



33) Does the application maintain a journal of transactions or snapshots of data between backup intervals?

34) Can the system administrator reconfigure to nonstandard port assignments other than the list of registered ports published by IANA?	☒ Yes	☐ N/A
Reference Information		

35) Does the application have the ability to run a backup concurrently with the operation of the application?	☒ Yes	☐ N/A
Reference Information		



36) Does the application include documentation that explains error messages to users and system administrators and the actions that are required?	☒ Yes	☐ N/A
☐ No		
Reference Information		

3.3 - Support Functionality

37) Briefly describe how this application is supported (i.e. onsite support, remote access, support, phone support, e-mail support, etc.)
Reference Information

3.3.1 - Security of Remote Support

38) Does your company utilize remote connection methods for technical support? (i.e. Dial-up, secure web tunneling, VPN client, Business-to-Business VPN using IPSec, etc) If yes, please explain.	☒ Yes	☐ N/A
☐ No		
Reference Information		



39) Is remote access a functionality that is built into the application itself?
If yes, please describe the security related with the remote access.

☒ Yes☐ N/A☐ No

Reference Information

40) If requested, can the application associate remote support activities with an individual employee of the vendor?

☒ Yes☐ N/A☐ No

Reference Information

41) If applicable, do vendor support personnel have specific roles and accesses that control access to ePHI within the application?

☒ Yes☐ N/A☐ No

Reference Information



42) Does the application audit remote support connection attempts and remote support actions such as application or configuration modifications?	☒ Yes	☐ N/A
☐ No		
Reference Information		

43) Does the application require remote access by the vendor for maintenance?	☒ Yes	☐ N/A
☐ No		
Reference Information		

3.3.2 - Protection from Malicious Code

44) Is the application compatible with commercial off the shelf (COTS) virus scanning software products for removal and prevention from malicious code? If no, indicate what additional security controls are included with the application/system used to mitigate the risks associated with malicious code.	☒ Yes	☐ N/A
☐ No		
Reference Information		



3.3.3 - Configuration Mgmt & Change Control

47) Can the operating system hosting the application (server or client) be updated by the user without voiding the application warranty or support agreement?
If no, please explain if operating systems changes, updates, and patches will be provided by the vendor.

☒ Yes ☐ N/A ☐ No



48) Describe how updates to the application are typically handled and how the application is certified to perform as intended with updates to the operating system and other helper applications (such as service packs and hot fixes and how the customer is notified)

Reference Information

49) Is OCHCA responsible for installing operating system or application security updates?
If no, describe how you typically install updates for your system/application and whether remote access would be required.

☒ Yes

☐ N/A

☐ No

Reference Information



3.4 - Vendor Info

3.4.1 - Service Level Agreements

50) Does your application come with a Service Level Agreement (SLA)? If yes, please describe any guaranteed response times associated with the SLA.		☒ Yes	☐ N/A
		☐ No	
Reference Information			

3.4.2 - Third Party Application Testing

51) Does your application undergo third-party application security testing? If so please describe the testing process and the frequency at which the testing is done.		☒ Yes	☐ N/A
		☐ No	
Reference Information			



52) Has the application been tested to be fully functional residing on its associated operating system/middleware platform configured with a recognized security configuration benchmark?
If yes, please indicate the benchmark.

☒ Yes☐ No☐ N/A

Reference Information

3.4.3 - Other

53) Can you provide references to other customers who have purchased your application/system?

☒ Yes☐ No☐ N/A

Reference Information



4.0 – Appendix

Authentication - The process of determining that an entity (someone or something) is the one claimed to be.

Authorization - The process of granting rights or access to systems, applications, or networks. Authorization determines who is trusted for a given purpose.

ePHI – Electronic Protected Health Information – Any information which is created or received, that relates to the past, present, or future physical or mental health or condition of an individual or can be used to identify an individual that is transmitted or stored on electronic media. *(Note: ePHI must be safeguarded to protect it from unauthorized disclosure)*

IANA – (Internet Assigned Numbers Authority, www.iana.org) The Internet body that was responsible for managing Internet addresses, domain names and protocol parameters. It has been superseded by ICANN (Internet Corporation for Assigned Names and Numbers), which was formed in 1998. IANA was chartered by the Internet Society (ISOC) and Federal Network Council (FNC) and has been located at and operated by the Information Sciences Institute at the University of Southern California

NTP/SNTP - (Network Time Protocol) A TCP/IP protocol used to synchronize the real-time clock in computers, network devices and other electronic equipment that is time sensitive.



ATTACHMENT A



County of Orange Health Care Agency Vendor Security Requirements

Application Service Provider Questionnaire

05/2010

Table of Contents

1.0 - Overview	3
2.0 - Vendor Instructions	3
2.1 - Example	3
3.0 - Questionnaire	4
3.1 - Vendor Contact Information.....	4
3.2.1 - Encryption	5
3.2.3 - Access Management.....	9
3.2.4 - Password/User Management	10
3.2.5 - Audit Capabilities	13
3.2.6 - Other Capabilities.....	16
3.3 - Support Functionality	17
3.3.1 - Security of Remote Support.....	17
3.3.2 - Protection from Malicious Code	19
3.3.3 - Configuration Mgmt & Change Control.....	20
3.4.1 - Service Level Agreements.....	22
3.4.2 - Third Party Application Testing	22
3.4.3 - Other.....	23
4.0 – Appendix	24



1.0 - Overview

The County of Orange Health Care Agency (OCHCA) requires that all vendors whose product falls within the realm of information technology meet a minimum set of functional and technical security requirements. As such, the Information Security Department has prepared a questionnaire that will help the IT staff more thoroughly understand the security ramifications related to the potential implementation of a vendor's product.

As part of the vendor approval process, the vendor must demonstrate compliance with the OCHCA's Vendor Security Requirements by responding in writing to the statements or questions listed in section three unless otherwise specified within the question. By responding to those statements or questions below, the Information Security department will be able to expedite the security approval process. Failure to respond to all statements and questions may result in your disqualification.

2.0 - Vendor Instructions

The OCHCA Information Security Department is looking for detailed, technical responses to the following statements and/or questions. The vendors should include any supporting documents including but not limited to security whitepapers, technical documents, security policies and/or procedures that you may have that will assist us in understanding your information security profile.

2.1 - Example

Insufficient Response: "Our product uses encryption."

Acceptable Response: "All communications between the clients and server are protected by through 128-Bit SSL encryption on TCP port 7443."

Each applicable section will include a reference section. If the question or statement relates to information referenced within your supporting documents, please provide the document name and page number within the associated reference section.



3.0 - Questionnaire

3.1 - Vendor Contact Information

Application Name:		Version:	Release Date:
Application Supports the following business functions:			
Vendor Representative Contact Information	Name:	Title:	Department:
	Company Name:	Telephone Number:	E-mail:
	Support Number:	Support E-mail:	Website URL:
Contracting Agency/ Department Contact Information	Department:		Telephone:
	Agency Contact:		E-Mail:
Additional Information:			



3.2 - Application Functionality

- 1) Briefly describe your application's function and indicate how the software functions (i.e. Client/Server, Web Based, etc.)

Reference Information

3.2.1 - Encryption

- 2) Does this application employ data encryption?
If no, continue to question 7.
If yes, describe whether it is network-based encryption, storage-based encryption, or both.

☐ Yes

☒ N/A

☐ No

Reference Information

- 3) Does the application encrypt data before sending it over the Internet or an open network?
If yes, indicate the type of encryption.

☐ Yes

☒ N/A

☐ No

Reference Information



- 4) Does the application encrypt data before storing on removable media such as backup tapes, CDs, DVDs, etc, or devices such as laptops, tablets, or computer workstation hard disk drives?
If yes, indicate the encryption used.

☒ Yes☐ N/A☐ No

Reference Information

- 5) Is password transmission and storage encrypted and un-viewable even to the system administrators?
If yes, indicate the encryption used.

☒ Yes☐ N/A☐ No

Reference Information



Application Service Provider
Questionnaire

Page 6

6) Is this application web-based or does this application include a web interface?
If no, continue to question 11.
If yes, include the types of secure connections that are supported.

☐ Yes	☒ N/A
☐ No	

	7) Is this application's web interface appropriate to deploy as Internet-facing? If no, please explain.	☐ Yes	☒ N/A
Reference Information			

8) Are there security safeguards are inherent in the application to protect against network vulnerabilities such as, but not limited to, SQL Injection, Cross Site Scripting, Website Defacement or Hijacking, installation of Trojan horses/spyware, etc.? If yes, please explain.	☐ Yes ☐ No	☒ N/A
Reference Information		



9) If this application is behind our perimeter firewall, are there protocols and IP ports need to be opened? If yes, please explain.	☐ Yes ☐ No	☒ N/A
Reference Information		

10) Should this application be protected by an application proxy? If so, please explain in detail.	☐ Yes ☐ No	☒ N/A
Reference Information		

11) Does this application/system have a typical network setup? Please include information like which network services would be required (i.e. DNS, SMTP, etc.)	☐ Yes ☐ No	☒ N/A
Reference Information		



3.2.3 - Access Management

12) Is the user authenticated to the application? If yes, briefly describe how the user is authenticated to the system. If no or not applicable, please continue to 25.	☐ Yes ☐ No	☒ N/A
Reference Information		

13) Does the application support integration with enterprise identity management systems? If yes, indicate the compatible systems (such as Directory Services, LDAP, Kerberos, etc.)	☐ Yes ☐ No	☒ N/A
Reference Information		

14) Is the application compatible with alternative authentication mechanisms (e.g. certificates, token, biometric, etc.?)	☐ Yes ☐ No	☒ N/A
Reference Information		



3.2.4 - Password/User Management

17) Can the user change their password at any time?

☒ Yes ☐ No ☐ N/A



18) Can the system administrator enforce password policy and/or complexity such as minimum length, numbers and alphabet requirements, and upper and lower case letters, etc.?

☐ Yes☒ N/A☐ No

Reference Information

19) Can the application force password expiration and prevent users from reusing a password?

☐ Yes☒ N/A☐ No

Reference Information

20) Can the application be set to automatically lock a user's account after a predetermined number of consecutive unsuccessful logon attempts?

☐ Yes☒ N/A☐ No

Reference Information



Application Service Provider
Questionnaire

Page 11

21) Does the application prohibit users from logging into the application on more than one workstation at the same time with the same user ID?

☐ Yes

☒ N/A

☐ No

Reference Information

22) Can the application be set to automatically log a user off the application after a predefined period of inactivity?

☐ Yes

☒ N/A

☐ No

Reference Information

23) Can the application support the removal of user's access privileges without requiring the deletion of the user account?

☐ Yes

☒ N/A

☐ No

Reference Information



Application Service Provider
Questionnaire

Page 12

3.2.5 - Audit Capabilities

26) Does this application capture user access activity such as successful logon, logoff, and unsuccessfully logon attempts? If yes, list the data elements contained in the audit log.	☐ Yes ☐ No	☒ N/A
---	---	--------------------------------------

Reference Information



27) Does this application capture data entries, changes, and deletions?
If yes, list the data elements contained in the audit log.

☐ Yes☒ N/A☐ No

Reference Information

28) Does the application time stamp for audit log entries synchronize with other applications and systems using NTP/SNTP?

☐ Yes☒ N/A☐ No

Reference Information

29) Can the audit log "data" be exported from the application for further processing (e.g. storage, analysis)?

☐ Yes☒ N/A☐ No

Reference Information



Application Service Provider
Questionnaire

Page 14

30) Are the audit log files protected from unauthorized alteration?
If yes, please describe the protections.

☐ Yes

☒ N/A

☐ No

Reference Information

31) Does the application allow a system administrator to set the inclusion or exclusion of audited events based on organizational policy and operating requirements or limits?

☐ Yes

☒ N/A

☐ No

Reference Information

32) Can the application continue normal operation even when the security audit capability is non-functional? (For example, if the audit log reaches capacity, the application should continue to operate and should suspend logging, start a new log, or begin overwriting the existing log)

☐ Yes

☒ N/A

☐ No

Reference Information



Application Service Provider
Questionnaire

33) Does the application maintain a journal of transactions or snapshots of data between backup intervals?

☐ Yes ☒ N/A ☐ No

34) Can the system administrator reconfigure to nonstandard port assignments other than the list of registered ports published by IANA?	☒ Yes	☒ N/A
	☐ No	
Reference Information		

35) Does the application have the ability to run a backup concurrently with the operation of the application?	☒ Yes ☐ No ☐ N/A
--	--



36) Does the application include documentation that explains error messages to users and system administrators and the actions that are required?	☐ Yes	☒ N/A
☐ No		
Reference Information		

3.3 - Support Functionality

37) Briefly describe how this application is supported (i.e. onsite support, remote access, support, phone support, e-mail support, etc.)
Reference Information

3.3.1 - Security of Remote Support

38) Does your company utilize remote connection methods for technical support? (i.e. Dial-up, secure web tunneling, VPN client, Business-to-Business VPN using IPSec, etc) If yes, please explain.	☐ Yes	☒ N/A
☐ No		
Reference Information		



39) Is remote access a functionality that is built into the application itself?
If yes, please describe the security related with the remote access.

☐ Yes

☒ N/A

☐ No

Reference Information

40) If requested, can the application associate remote support activities with an individual employee of the vendor?

☐ Yes

☒ N/A

☐ No

Reference Information

41) If applicable, do vendor support personnel have specific roles and accesses that control access to ePHI within the application?

☐ Yes

☒ N/A

☐ No

Reference Information



43) Does the application require remote access by the vendor for maintenance?		☐ Yes	☒ N/A
		☐ No	
Reference Information			

44) Is the application compatible with commercial off the shelf (COTS) virus scanning software products for removal and prevention from malicious code? If no, indicate what additional security controls are included with the application/system used to mitigate the risks associated with malicious code.	☐ Yes ☐ No	☒ N/A
Reference Information		



45) Does the application's client software operate without requiring the user to have local administrator level rights in order to run the application?

☐ Yes

☒ N/A

☐ No

Reference Information

3.3.3 - Configuration Mgmt & Change Control

46) Are updates to the application software and/or the operating system controlled by a mutual agreement between the support vendor and the application owner?

☐ Yes

☒ N/A

☐ No

Reference Information

47) Can the operating system hosting the application (server or client) be updated by the user without voiding the application warranty or support agreement?
If no, please explain if operating systems changes, updates, and patches will be provided by the vendor.

☐ Yes

☒ N/A

☐ No

Reference Information



48) Describe how updates to the application are typically handled and how the application is certified to perform as intended with updates to the operating system and other helper applications (such as service packs and hot fixes and how the customer is notified)

Reference Information

49) Is OCHCA responsible for installing operating system or application security updates?
If no, describe how you typically install updates for your system/application and whether remote access would be required.

☐ Yes

☒ N/A

☐ No

Reference Information



3.4 - Vendor Info

3.4.1 - Service Level Agreements

50) Does your application come with a Service Level Agreement (SLA)? If yes, please describe any guaranteed response times associated with the SLA.		☐ Yes	☒ N/A
		☐ No	
Reference Information			

3.4.2 - Third Party Application Testing

51) Does your application undergo third-party application security testing? If so please describe the testing process and the frequency at which the testing is done.		☐ Yes	☒ N/A
		☐ No	
Reference Information			



52) Has the application been tested to be fully functional residing on its associated operating system/middleware platform configured with a recognized security configuration benchmark?
If yes, please indicate the benchmark.

☐ Yes
☐ No

☒ N/A

Reference Information

3.4.3 - Other

53) Can you provide references to other customers who have purchased your application/system?

☐ Yes
☐ No

☒ N/A

Reference Information



Application Service Provider
Questionnaire

Page 23

4.0 – Appendix

Authentication - The process of determining that an entity (someone or something) is the one claimed to be.

Authorization - The process of granting rights or access to systems, applications, or networks. Authorization determines who is trusted for a given purpose.

ePHI – Electronic Protected Health Information – Any information which is created or received, that relates to the past, present, or future physical or mental health or condition of an individual or can be used to identify an individual that is transmitted or stored on electronic media. *(Note: ePHI must be safeguarded to protect it from unauthorized disclosure)*

IANA – (Internet Assigned Numbers Authority, www.iana.org) The Internet body that was responsible for managing Internet addresses, domain names and protocol parameters. It has been superseded by ICANN (Internet Corporation for Assigned Names and Numbers), which was formed in 1998. IANA was chartered by the Internet Society (ISOC) and Federal Network Council (FNC) and has been located at and operated by the Information Sciences Institute at the University of Southern California

NTP/SNTP - (Network Time Protocol) A TCP/IP protocol used to synchronize the real-time clock in computers, network devices and other electronic equipment that is time sensitive.



Question and Answers for Bid #042CDMFY10037 - Adult Custody Medical Specialty Telemedicine Pilot Project

OVERALL BID QUESTIONS

There are no questions associated with this bid. If you would like to submit a question, please click on the "Create New Question" button below.

Question Deadline: Jun 14, 2010 4:00:00 PM PDT