COUNTY OF SANTA CLARA, CALIFORNIA

REQUEST FOR PROPOSAL # FMP01 082010
FOR
FILE MAKER PRO TECHNICAL SUPPORT

ISSUED:
AUGUST 16, 2010

PROPOSALS DUE:
SEPTEMBER 10, 2010 BY 3:00 P.M. PACIFIC TIME

SANTA CLARA VALLEY HEALTH & HOSPITAL SYSTEM
2325 ENBORG LANE, SECOND FLOOR IS
SAN JOSE, CA 95128

CONTACT: CHERI SILVEIRA
408.885.6490
Cheri.silveira@hhs.sccgov.org

Conference Room Information for Pre-Proposal Conference
County of Santa Clara Procurement Department
2310 North First Street, Suite 201, ***Cedar Conference Room***
San Jose, CA 95131

Conference Call Information for Pre-Proposal Conference
Participants Dial **1-866-249-5279 and Enter Access Code 559951**

TABLE OF CONTENTS

I. INTRODUCTION

A. INVITATION

The County of Santa Clara (hereafter, "County") is requesting proposals from qualified suppliers to provide File Maker Pro database support services for the Santa Clara Valley Health & Hospital System (SCVHHS) Chronic Care Registry. Support for the FileMaker Pro is needed to ensure platform stability, meet the growing clinical data needs, and support the various chronic care programs within Santa Clara Valley Medical Center (VMC).

Registry tools assist clinicians in providing optimal care to their patients, particularly for patients with chronic care needs. These tools can also be used to provide clinicians and administrators with quality and dashboard data. FileMaker Pro is a chronic care disease registry application used to support chronic care programs including diabetes center, Protime clinic, pediatric asthma clinic, stroke program, medical home and PHASE program at Silver Creek clinic with expansion to other clinic sites. The FileMaker Pro database interfaces with Lab, Pharmacy and other HHS source applications. Over the years, FileMaker Pro has grown in usage and supports the medical home model expansion.

The database support required as part of this request includes:

Contracted services will take place on site at various clinics on the SCVHHS campus, where the FileMaker Pro database is being utilized. The following describes services required:

1. **Database Support and Maintenance shall consist of:**
   - Technical assistance support to staff between the hours of 8:00am – 5:00pm
   - Daily file upload from one server to another
   - Troubleshooting and resolving system issues
   - Repairing the existing FileMaker Pro database including telephone support for the following departments:
     Protime Clinic
     Diabetes and Metabolism Center
     Stroke
     CHF
     Pediatric Healthy Lifestyle Center
     Pediatric Tuberculosis
     Valley Health Centers including Sunnyvale, Bascom, Moorpark, Gilroy, East Valley, Tully and Silver Creek
   - Upgrading FileMakerPro client version from version 9.0 to 10.0 or applicable version
   - Upgrading FileMakerPro Server from version 9.0 to FileMaker Server 10 or applicable version
   - Configuration of database for full HIPAA compliance

   Telephone support shall be provided with a response time of one business day.

2. **Interface Automation**
   - Coordinate and work with Information Systems department to build system interfaces with chronic care registry including the development of validation rules

3. **Training Services**
   Individual training services for the purpose of upgrading an employee's skill level in order to maintain the FileMaker Pro database. All user training will occur on site.

4. Meetings with staff including departmental meetings to learn SCVHHS database structure and interfaces

5. Query development and generation of reports as needed to support chronic care programs and services

This RFP shall result in a single source award.

B. BACKGROUND

1. Santa Clara Valley Health and Hospital System

Santa Clara Valley Health and Hospital System (SCVHHS) is a 24-hour healthcare facility providing healthcare to approximately 80,000 patients in Santa Clara County. SCVHHS is comprised of: The Valley Medical Center (VMC), VMC Ambulatory and Managed Care, Valley Specialty Center (VSC), Valley Health Center (VHC), Valley Health Plan (VHP), Public Health Department (PH), Department of Alcohol and Drug Services (DADS), Mental Health Department (MH), Children's Shelter and Custody Health Services (CSCHS), and Community Outreach Programs.

2. Santa Clara Valley Medical Center (SCVMC)

SCVMC is a 574-bed acute care public teaching and safety-net hospital owned and operated by Santa Clara County. SCVMC provides advanced services including a world-class Rehabilitation Center, Regional Burn Center, High-Risk Maternity program, and Trauma Center. The teaching program is affiliated with Stanford University Medical School. SCVMC provides a full range of inpatient, emergency, rehabilitation, neonatal, intensive care, high-risk maternity care, psychiatry, pediatric intensive care, and burn intensive care services. SCVMC is one of three designated trauma centers in the county, and operates a comprehensive emergency room.

3. SCVMC Ambulatory and Managed Care

The Ambulatory and Managed Care Department at Santa Clara Valley Medical Center provides an extensive array of healthcare services through a network of seven neighborhood health centers supported by four mobile health and dental service units.

DESCRIPTION	TOTAL
Number of Licensed Beds	574
IP Admits & Psychiatry 2008	29,931
IP Average Length of Stay 2008	4.84 Days

4. Ambulatory and Managed Care (AMC)

Ambulatory and Community Health Services provides an extensive array of healthcare services through a network of ten neighborhood Health Centers supported by four mobile health and dental service units. The Health Centers are located through out Santa Clara

County and offer Pediatric, Obstetric/Gynecology, Adult Medicine, Geriatric, Sub-specialty, Dental, and Urgent care services. Sites include Valley Health Center Moorpark, Tully, San Martin, East Valley, Moorpark, Fair Oaks, Silver Creek, Lenzen, and Bascom.

a. Ambulatory and Managed Care Statistics

DESCRIPTION	TOTAL
Number of patients	200,000
Number of visits for FY09	670,147
Attending Physicians	350

5. Valley Connections Call Center

Valley Connection Call Center at Santa Clara Valley Medical Center is responsible handling a large volume of inbound calls using an ACD, and making a large volume of outbound calls using an IVR. There are a number of agencies and departments that are linked via a T1 circuit to the ACD. The hours of operation are 24 x 7, 365 days a year.

a. Valley Connection Statistics

DESCRIPTION	TOTAL
Number of Inbound ACD calls received per month	~ 80,000 – 85,000
Clerical Calls per month	~ 39,000 – 42,000
RN Calls per month	~ 2,150 – 2,600
Number of Insurance calls on a Monday	4,137
Number of calls in 11 different languages	36,924 (2 weeks in July 2009)
Number of calls for Physicians	~ 150 per week (5 languages)

6. Valley Health Plan (VHP)

Valley Health Plan is a Santa Clara County owned and operated Knox Keene licensed Health Maintenance Organization (HMO). VHP offers commercial medical insurance coverage to County employees, retirees and individual conversions, Council on Aging, First Five Commission, Valley Transit Authority, and In Home Support Service Workers.

DESCRIPTION	TOTAL
Enrollment	57,000
Staff: • Medical Directors • Utilization Review Coordinators • Administrative Support Staff • Contracts and Marketing • Claims Personnel • Member Services Personnel	 4 4 2 2 5 5

DESCRIPTION	TOTAL
	TOTAL: 17 FTEs

7. Information Services Department

Information systems and technology for SCVHHS is centralized in the Information Services (IS) Department and is responsible for all systems, planning, development and support within HHS. Business units comprising IS are:

A. Application Services – provides a comprehensive array of services
- Strategy
- Solutions
- Sourcing
- Support

B. Technical Services
- Data Center Operations
- Operations
- Customer Service
- Field Support

8. Technical Environment

SERVER

Operating system	Windows Server 2003/Windows Active Directory, Linux
Hardware	Intel Dual Core 3.0 GHZ – 2MB cache, fiber/GBE NIC (redundant), SAN integration via Emulex 1000-L2 HBAs, dual processor, 4GB RAM per processor minimum, redundant power supplies. Blade technology preferred
Backup	CA ARCServe
Server redundancy/cluster	Depends on application
Disk array	Raid 1(Blade),Standalone: RAID 1 (OS) RAID 5 (Data)
Antivirus	Symantec AV 10.x

DESKTOP/LAPTOP HARDWARE

Mid-level PC with 19” monitor	HP Convertible Minitower For most current spec see Valley Pages – Forms – Information Services – HHS Special Specifications
Small footprint PC with flat 19” LCD panel monitor (where space requires small footprint)	HP Ultra-slim Desktop For most current spec see Valley Pages – Forms – Information Services – HHS Special Specifications
Monitor settings	1024 x 768/ high color
Laptop	HP NC8430 – 15.4” display, Wi-Fi a/g/n For most current spec see Valley Pages – Forms – Information Services – HHS Special Specifications
Docking station	Basic docking station 1.1

DESKTOP/LAPTOP SOFTWARE

Operating System	Windows XP with Service Pack 3
Office applications	Microsoft Office 2003 Professional, sp2
Email	Microsoft Outlook 2003
Terminal emulation	NetManage Rumba 2000 v.6
PDF reader	Adobe Acrobat Reader 7.0
Desktop database	Microsoft Access 2003
Internet browser	Microsoft Internet Explorer 7.0
Antivirus	Symantec AntiVirus Corporate Edition Version 11.x
Java	Java Version 1.5.x
Encryption – ***Laptop Only***	PointSec v6.1

PRINTERS

Laser	HP LaserJet – Group - Mid-range printer is 4250tn HP Laserjet – MFP is HP 4345tn HP Laserjet – standalone is HP2105d
Impact	Not supported
Label	Zebra with network connectivity
Network interface	HP- Internal Jet Direct

COMMUNICATION

Protocol	TCP/IP
Topology	Ethernet
Routers/ switches	Cisco
Bandwidth – network	Gigabit (sx/lx)
Bandwidth – to the desktop	10/100/1000 MB/ second
Backbone	Fiber optic
Cable to the desktop	Category 5e UTP with RJ45 connections

REMOTE AUTHENTICATION/SUPPORT

Point to Point SSL VPN or CRYPTOcard via Cisco VPN

9. File Maker Pro

Current Version	Version 6 for one clinic, 10 for others
Number of tables	Approximately 200
Number of concurrent user licenses	40
Number of interfaces	20

C. PROJECT SCOPE OF WORK

The File Maker Pro database support may consist of planning; organizing and implementing changes to the current File Maker Pro database that includes technical assistance, interface building, support, and maintenance, repairing the database if needed, upgrading to current versions, training staff, and attending meetings as required.

D. POINT OF CONTACT:

The County has designated a Procurement Officer who is responsible for the conduct of this procurement whose name, address and telephone number is listed below:

Cheri Silveira, IS Manager
Santa Clara Valley Health & Hospital System
2325 Enborg Lane, Second Floor
San Jose, CA 95128
Telephone: 408.885.6490 or Fax: 408.885.2036
E-mail: cheri.silveira@hhs.sccgov.org

Any inquiries or request regarding this procurement must be submitted to the Procurement Officer in writing. Offerors may contact ONLY the Procurement Officer regarding this procurement. Other County employees do not have the authority to respond on behalf of the County.

II. CONDITIONS GOVERNING THE PROCUREMENT

This section of the RFP contains the anticipated schedule for the procurement and describes the procurement events as well as the conditions governing the procurement.

A. SEQUENCE OF EVENTS AND CONTACT INFORMATION

The Procurement Officer will make every effort to adhere to the following anticipated schedule:

	Action	Date
1.	Issue of RFP	**August 16, 2010**
2.	Deadline To Submit Written Questions	**August 19, 2010 3:00 P.M. PT**
3.	Pre-Proposal Conference	**August 24, 2010 at 1:00 P.M. PT**
4.	Response to Written or Pre-Proposal Questions/RFP Addendum	August 26, 2010
5.	Submission of Proposals	**September 10, 2010 3:00 P.M. PT**
6.	Proposal Evaluation	September 13, 2010 – September 24, 2010
7.	Selection of Shortlist	September 28, 2010
8.	Demonstrations/presentations (County option)	Week of October 4, 2010
9.	Selection of Finalist for Negotiations	October 12, 2010
10.	Final Negotiations, BAFO, and finalize and award contract	November 1, 2010
11.	Commencement of Contract	November 15 2010

B. EXPLANATION OF EVENTS

1. ISSUE OF RFP

This RFP is being issued by the Santa Clara Valley Health & Hospital System Information Services Department. Copies of this RFP including supporting documents may be obtained from Bidsync's web site at http://www.bidsync.com.

2. PRE-PROPOSAL CONFERENCE

A pre-proposal conference is scheduled for this RFP on August 24, 2010 at 1:00 P.M. Please submit all questions by the due date specified in paragraph A of section II. See below for information on how to access the conference:

Conference Room Information for Pre-Proposal Conference
County of Santa Clara Procurement Department
2310 North First Street, Suite 201, ***Cedar Conference Room***
San Jose, CA 95131

Conference Call Information for Pre-Proposal Conference
Participants Dial **1-866-249-5279 and Enter Access Code 559951**

3. DEADLINE TO SUBMIT WRITTEN QUESTIONS

FOR QUESTIONS DUE ON AUGUST 19, 2010, PLEASE CHERI SILVEIRA

at cheri.silveira@hhs.sccgov.org, 408.885.6490

Potential Offerors may submit written questions to this RFP until the deadline as indicated in Section II, Paragraph A. The Procurement Officer will not respond to questions submitted in any other manner or format.

Answers to questions received by the deadline will be listed on an addendum to the RFP and posted on the bid management site http://www.bidsync.com. Additional written questions must be received by the Procurement Officer no later than two (2) days after the addendum is posted. The County will respond in the same manner. Thereafter, the County does not guarantee that questions submitted will be responded to before the RFP closing date and time.

4. RESPONSE TO WRITTEN QUESTIONS/RFP AMENDMENTS

Written responses to written questions, and any changes to the RFP, will be issued as an addendum, and posted on http://www.bidsync.com. The County reserves the right to post addenda until the RFP closing date and time.

5. SUBMISSION OF PROPOSAL

PROPOSALS MUST BE RECEIVED **NO LATER THAN THE DEADLINE SPECIFIED IN PARAGRAPH A, OF SECTION II.** Proposals are to be received at the place listed below. All received proposals will be time stamped.

All deliveries via express carrier should be addressed as follows:

Cheri Silveira, IS Manager – RFP **FMP01 082010**
Santa Clara Valley Health & Hospital System
Information Services
2325 Enborg Lane, Second Floor
San Jose, CA 95128

Proposals must be sealed and labeled on the outside of the package to clearly indicate that they are in response to the RFP # and title as referenced on the cover page.

6. DEMONSTRATION/PRESENTATIONS

At County option, Offerors on the short list may be required to perform a demonstration/presentation of their proposed solution. Demonstrations/presentations will be held on-site at a County location. Date, time, and location to be determined.

C. GENERAL

1. INCURRING COST

This RFP does not commit the County to award, nor does it commit the County to pay any cost incurred in the submission of the Proposal, or in making necessary studies or designs for the preparation thereof, nor procure or contract for services or supplies. Further, no reimbursable cost may be incurred in anticipation of a contract award.

2. CLAIMS AGAINST THE COUNTY

Neither your organization nor any of your representatives shall have any claims whatsoever against the County or any of its respective officials, agents, or employees arising out of or relating to this RFP or these procedures (other than those arising under a definitive Agreement with your organization in accordance with the terms thereof).

3. GUARANTEE OF PROPOSAL

Responses to this RFP, including proposal prices, will be considered firm and irrevocable for one-hundred and eighty (180) days after the due date for receipt of proposals and/or one-hundred eighty (180) days after receipt of a best and final offer, if one is submitted.

4. BASIS FOR PROPOSAL

Only information supplied by the County in writing by the Procurement Officer in connection to this RFP should be used as the basis for the preparation of Offeror's proposal.

5. FORM OF PROPOSALS

No oral, telephone, facsimile, or electronic proposals will be accepted.

6. AMENDED PROPOSAL

An Offeror may submit an amended proposal before the deadline for receipt of proposals. Such amended proposals must be complete replacements for a previously submitted proposal and must be clearly identified as such in the transmittal letter. The County personnel will not merge, collate, or assemble proposal materials.

7. WITHDRAWAL OF PROPOSAL

Offerors will be allowed to withdraw their proposals at any time prior to the deadline for receipt of proposals. The Offeror must submit a written withdrawal request signed by the Offeror's duly authorized representative addressed to the Director of Procurement and submitted to the Procurement Officer.

8. LATE RESPONSES

All proposals submitted in response to this RFP must be delivered in person or received via courier or mail no later than the RFP due date and time. The Procurement Department time and date stamp will be the basis of determining receipt of proposal. Late responses will not be considered.

9. NO PUBLIC PROPOSAL OPENING

There will be no public opening for this RFP.

10. CALIFORNIA PUBLIC RECORDS ACT (CPRA)

All proposals become the property of the County, which is a public agency subject to the disclosure requirements of the California Public Records Act ("CPRA"). If Contractor proprietary information is contained in documents submitted to County, and Contractor

claims that such information falls within one or more CPRA exemptions, Contractor must clearly mark such information "CONFIDENTIAL AND PROPRIETARY," and identify the specific lines containing the information. In the event of a request for such information, the County will make best efforts to provide notice to Contractor prior to such disclosure. If Contractor contends that any documents are exempt from the CPRA and wishes to prevent disclosure, it is required to obtain a protective order, injunctive relief or other appropriate remedy from a court of law in Santa Clara County before the County's deadline for responding to the CPRA request. If Contractor fails to obtain such remedy within County's deadline for responding to the CPRA request, County may disclose the requested information.

Contractor further agrees that it shall defend, indemnify and hold County harmless against any claim, action or litigation (including but not limited to all judgments, costs, fees, and attorneys fees) that may result from denial by County of a CPRA request for information arising from any representation, or any action (or inaction), by the Contractor.

11. CONFIDENTIALITY

All data and information obtained from the County by the Offeror and its agents in this RFP process, including reports, recommendations, specifications and data, shall be treated by the Offeror and its agents as confidential. The Offeror and its agents shall not disclose or communicate this information to a third party or use it in advertising, publicity, propaganda, or in another job or jobs, unless written consent is obtained from the County. Generally, each proposal and all documentation, including financial information, submitted by an Offeror to the County is confidential until a contract is awarded, when such documents become public record under state and local law, unless exempted under CPRA.

12. ELECTRONIC MAIL ADDRESS

Most of the communication regarding this procurement will be conducted by electronic mail (e-mail). Potential Offerors agree to provide the Procurement Officer with a valid e-mail address to receive this correspondence.

13. USE OF ELECTRONIC VERSIONS OF THE RFP

This RFP is being made available by electronic means. If accepted by such means, the Offeror acknowledges and accepts full responsibility to insure that no changes are made to the RFP. In the event of conflict between a version of the RFP in the Offeror's possession and the version maintained by the Procurement Department the version maintained by the Procurement Department must govern.

14. COUNTY RIGHTS

The County reserves the right to do any of the following at any time:

a. Reject any or all proposal(s), without indicating any reason for such rejection;
b. Waive or correct any minor or inadvertent defect, irregularity or technical error in a proposal or the RFP process, or as part of any subsequent contract negotiation;
c. Request that Offerors supplement or modify all or certain aspects of their proposals or other documents or materials submitted;
d. Terminate the RFP, and at its option, issue a new RFP;
e. Procure any equipment or services specified in this RFP by other means;

f. Modify the selection process, the specifications or requirements for materials or services, or the contents or format of the proposals;
g. Extend a deadline specified in this RFP, including deadlines for accepting proposals;
h. Negotiate with any or none of the Offerors;
i. Modify in the final agreement any terms and/or conditions described in this RFP;
j. Terminate failed negotiations with an Offeror without liability, and negotiate with other Offerors;
k. Disqualify any Offeror on the basis of a real or apparent conflict of interest, or evidence of collusion that is disclosed by the proposal or other data available to the County;
l. Eliminate, reject or disqualify a proposal of any Offeror who is not a responsible Offeror or fails to submit a responsive offer as determined solely by the County; and/or
m. Accept all or a portion of an Offeror's proposal.

III. RESPONSE FORMAT AND ORGANIZATION

This section contains relevant information Offerors should use for the preparation of their proposals.

A. NUMBER OF RESPONSES

Offerors must submit only one proposal.

B. ORIGINAL AND COPIES

Offerors must provide one (1) original and four (4) identical copies of their proposal to the location specified on or before the closing date and time for receipt of proposals.

The original binder must be stamped “original” and contain original signatures on the necessary forms. The remaining sets should be copies of the originals.

Offerors must also provide one (1) electronic copy of their proposal in CD-ROM format, prepared using Microsoft Office 2003 (Word, Excel and Project). The CD shall be included in the original binder.

C. PROPOSAL FORMAT

All proposals shall be typewritten on standard 8 ½ x 11 paper (larger paper is permissible for charts, spreadsheets, etc.) and placed within a binder with tabs delineating each section. Hard copies should utilize both sides of the paper where practical.

1. LETTER OF TRANSMITTAL

Each proposal received must include a letter of transmittal. The letter of transmittal **MUST**:

a. Identify the submitting organization;
b. Identify the name, title, telephone and fax numbers, and e-mail address of the person authorized by the organization to contractually obligate the organization;
c. Identify the name, title, telephone and fax numbers, and e-mail address of the person authorized to negotiate the contract on behalf of the organization;
d. Identify the names, titles, telephone and fax numbers, and e-mail addresses of persons to be contacted for clarification;
e. Be signed by the person authorized to contractually obligate the organization; and
f. Acknowledge receipt of any and all addenda to this RFP; and identify all sections of the proposal that the Offeror claims contain “proprietary” or “confidential” information.

2. PROPOSAL ORGANIZATION

The proposal must be organized and indexed in the following format and must contain, at a minimum, all listed items in the sequence indicated:

Tab 1: Letter of Transmittal
Tab 2: Table of Contents
Tab 3: Executive Summary
Tab 4: Section V – A: Offeror’s Corporate Information, items 1 – 6
Tab 5: Section V – B: Functional Requirements

Appendix A: Database Support,Training, and Ongoing Support for File Maker Pro
Appendix C: Non-collusion Declaration Form
Appendix D: Declaration of Local Business, if applicable.
AppendixE: Vendor Remote Access and User Responsibility forms, if applicable

Tab 6: Appendix F: Offeror's Terms and Conditions
Insurance Declaration to meet the Insurance Requirements
Financial Statements (as applicable)

Appendix B - Proposal Cost Response Form: the original form must be submitted in a sealed envelope marked "Original Appendix B." In addition, submit four (4) copies in a separate sealed envelope marked "Copies of Appendix B."

3. PROPOSAL PREPARATION INSTRUCTIONS

Within each section of their proposal, Offerors should address the items in the order in which they appear in this RFP. All forms provided in the RFP shall be thoroughly completed and included in the appropriate section of the proposal.

IV. EVALUATION

A. FACTORS

The **Evaluation Criteria** listed below will be utilized in the evaluation of the Offeror's written proposals and demonstration/presentation accordingly. The expectation is that those proposals in the competitive range may be considered for contract award. The proposal should give clear, concise information in sufficient detail to allow an evaluation based on the criteria below. An Offeror must be acceptable in all criteria for a contract to be awarded to that Offeror whose proposal provides the best value to the County.

1. Corporate strength, experience, financial strength, references and reputation of Offeror;
2. Ability to meet business, technical and functional requirements;
3. Methodology for database support, training, and ongoing support; and
4. Local Preference.

The overall total cost to the County will be considered and the degree of the importance of cost will increase with the degree of equality of the proposals in relation to the other factors on which selection is to be based.

B. LOCAL BUSINESS PREFERENCE

In accordance with applicable sections of Board Policy, Section 5.3.13, in the formal solicitation of goods or services, the County of Santa Clara shall give responsive and responsible Local Businesses the preference described below.

"Local Business" means a lawful business with a physical address and meaningful "production capability" located within the boundary of the County of Santa Clara.

The term "production capability" means sales, marketing, manufacturing, servicing, or research and development capability that substantially and directly enhances the firm's or bidder's ability to perform the proposed contract. Post Office box numbers and/or residential addresses may not be used as the sole bases for establishing status as a "Local Business."

In the procurement of goods or services in which best value is the determining basis for award of the contract, five percent (5%) of the total points awardable will be added to the Local Business score.

When a contract for goods or services, as defined in this policy, is presented to the Board of Supervisors for approval, the accompanying transmittal letter shall include a statement as to whether the proposed vendor is a Local Business, and whether the application of the local preference policy was a decisive factor in the award of the proposed contract.

This Local Business preference shall not apply to the following:

1. Public works contracts,
2. Where such a preference is precluded by local, state or federal law or regulation,
3. Contracts funded in whole or in part by a donation or gift to the County where the special conditions attached to the donation or gift prohibits or conflicts with this preference policy. The donation or gift must be approved or accepted by the Board of Supervisors in accordance with County policy, or

4. Contracts exempt from solicitation requirements under an emergency condition in accordance with board policy, state law and/or the County of Santa Clara Ordinance Code (Section A34-82).

In order to be considered for Local Preference, proposer must complete and submit Declaration of Local Business with its RFP response.

V. OFFEROR SUBMITTAL

This section contains requirements and relevant information Offerors should use for the preparation of their proposals. Offerors should thoroughly respond to each requirement.

A. OFFEROR'S CORPORATE INFORMATION

1. EXECUTIVE SUMMARY

Include an executive summary which should be a one or two page summary intended to provide the Evaluation Committee with an overview of the significant business features of the proposal.

2. OFFEROR EXPERIENCE/INFORMATION

The Offeror shall include in their proposal a statement of relevant experience. The Offeror should thoroughly describe, in the form of a narrative, its experience and success as well as the experience and success of subcontractors, if applicable in providing and/or supporting the proposed system.

In addition Offerors are required to provide the following information:

a. Offerors shall provide the company name, business address, including headquarters, all local offices, co-location locations (city/state), and telephone numbers.

b. Offerors shall provide the length of time they have been providing File Maker Pro support and training including interface automation.

c. Offerors shall indicate any offices or facilities located within the County of Santa Clara that substantially and directly enhances the Offeror's ability to perform the proposed contract.

d. Offerors shall provide a description of the Offeror's organization, including names of principals, number of employees, client base, areas of specialization and expertise, and any other information that will assist the Evaluation Committee in formulating an opinion about the stability and strength of the organization.

e. Offerors shall provide the name of the jurisdiction in which the Offeror is organized and the date of such organization.

f. Offerors shall provide specifics on the number of certified local (stationed in greater Bay Area) technicians.

g. Offerors shall provide a description of the depth of their experience with providing File Maker Pro support services

h. Offeror shall describe the method used for change management and advance notification timeframe for application changes.

i. Offeror shall describe the data security guarantee (data encryption, data mining, and data mismanagement penalties (leakage, etc.).

j. Provide a complete disclosure if Offeror, its subsidiaries, parent, other corporate affiliates, or subcontractors have defaulted in its performance on a contract during the past five years which has led the other party to terminate the contract. If so, identify the parties involved and the circumstances of the default or termination.

k. A list of any lawsuits filed against the Offeror, its subsidiaries, parent, other corporate affiliates, or subcontractors in the past five years and the outcome of those lawsuits. Identify the parties involved and circumstances. Also, describe any civil or criminal litigation or investigation pending.

3. FINANCIAL STABILITY/OFFEROR FINANCIAL INFORMATION

Offeror shall submit copies of the most recent years independently audited financial statements, as well as those for the preceding three years, if they exist. The submission shall include the audit opinion, balance sheet, income statement, retained earnings, cash flows, and notes to the financial statements. If independently audited financial statements do not exist for the Offeror, the Offeror shall state the reason and, instead, submit sufficient information such as the latest Dun and Bradstreet report to enable the Evaluation Committee to determine the financial stability of the Offeror. The Management Analyst may request and the Offeror shall supply any additional financial information requested in a timely manner.

4. PAST PERFORMANCE (REFERENCES)

The Offeror's proposal shall include three different external references from clients who have completed their projects in the last three years, who are willing to validate the Offeror's past performance on similar projects of size and scope. The minimum information that shall be provided for each client reference follows:

1. Name of the contact person;
2. Name of the company or governmental entity;
3. Address of the contact person;
4. Telephone number of contact person;
5. Email address of the contact person;
6. A description of the services provided and dates the services were provided;

5. INDEMNITY AND INSURANCE REQUIREMENTS

Offerors shall provide a certificate(s) of insurance or a copy of the insurance declaration page(s) with their proposals as written evidence of their ability to meet the insurance certificate and other applicable County insurance requirements in accordance with the provisions listed in Attachment B of the RFP. In addition, Offerors should provide a letter from an insurance agent or other appropriate insuring authority documenting their willingness and ability to endorse their insurance policies making the County an additional insured.

6. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT AND HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT

Explain if your proposed system meets the Health Insurance Portability and Accountability Act requirements and Health Information Technology for Economic and Clinical Health Act Business Associate Requirements (Attachment C).

B. FUNCTIONAL REQUIREMENTS

The County is seeking a contractor to provide a complete solution to satisfy the technical, functionality, and integration requirements and one who is capable of providing the stated capacity and service levels as well as the training and technical support required to maintain the File Maker Pro database in an operational status. Provide a detailed response on how the Offeror will fulfill the requirements of the County.

C. COST PROPOSAL (APPENDIX B)

Offerors shall complete all pages of the Proposal Cost Response Form and submit it in a sealed envelope with their proposal. The proposed costs shall directly relate to the Project Work Plan.

D. OTHER SUBMITTALS

1. NON-COLLUSION DECLARATION (APPENDIX C)

Offerors shall complete and submit Non-collusion Declaration form with their proposal.

2. DECLARATION OF LOCAL BUSINESS (APPENDIX D)

Offerors shall complete and submit Declaration of Local Business form with their proposal, if applicable.

4. VENDOR REMOTE ACCESS AND USER RESPONSIBILITY (APPENDIX E)

Offeror shall complete and submit the Vendor Remote Access and User Responsibility form with proposal, if applicable.

5. OFFEROR'S TERMS AND CONDITIONS (APPENDIX F)

Should Offerors object to any of the County's terms and conditions listed in Attachment A, Offerors must propose specific alternative language and indicate the reason for their objection. The County may or may not accept the alternative language. General references to the Offeror's terms and conditions or attempts at complete substitutions are not acceptable to the County. Offerors must provide a brief discussion of the purpose and impact, if any, of each proposed changed followed by the specific proposed alternate wording.

In addition, Offerors must submit with their proposal any additional terms and conditions that they expect to have included in the contract negotiated with the County. Offerors must provide specific proposed wording and a brief discussion of the purpose and impact, if any. Include any applicable agreement, such as license, service level, maintenance, etc.

APPENDIX A

DATABASE SUPPORT, TRAINING, AND ONGOING SUPPORT FOR FILE MAKER PRO

1. Database Support

a. Include the database support plan that the Offeror intends to employ for the project and an explanation of how it will support the support requirements and logically lead to the required deliverables. The description shall include the organization of the project team, including accountability and lines of authority.

b. Describe services to be provided to ensure success of the database support e.g. publicize the system to employees, organizing support infrastructure and processes, consulting on content set up and management etc.

c. Describe how the relationship between the County and Offeror will be managed from an account and technical support perspective.

d. Describe what is required of the County to ensure the successful support of File Maker Pro.

e. Include the steps that will be undertaken to identify and resolve any issues or problems before, during and after the support engagement.

f. Include a list of proposed project staff and key personnel.

g. Provide resumes, experience narratives and at least one reference for key personnel who will be assigned to the project, if awarded the contract.

h. Explain the relationship of the database support team with the Offeror, including job title and years of employment with the Offeror; role to be played in connection with the proposal; relevant certifications and experience.

2. Statement of Work (SOW) - Training Plan

a. Include a description for training for two different audiences:

   i. Power users/administrators and technical administrators.
   ii. General users.

b. Describe the type and quantity of training that will be provided for each audience. The description must include:

   i. A recommended training curriculum for on-site training;
   ii. Explain how the Offeror will work with the County to determine training needs and tailor the curriculum;

c. Describe the training facility requirements for physical layout, communication needs (internet connectivity, etc), projectors, # of computers, etc that are needed to fulfill the proposed training plan. Identify which elements of the training facility will be supplied by the Offeror.

3. SOW - Project Work Plan

Include a detailed work plan for the database support tasks noted in the Invitation section.

a. **Task Level -**The plan shall include all activities necessary for a successful project down to the task level.

b. **Identify All Resources -** The plan shall clearly identify all Offeror (including subcontractors) and using agency resources required to successfully complete the project. Provide job descriptions and the number of personnel to be assigned to tasks supporting implementation of the project. Identify County resources needed for each task.

c. **Deliverables** – describe the deliverables of each task.

d. **Time lines** – describe the timeline of each task.

e. **Acceptance criteria** – describe the criteria used to determine completion of each task.

f. **Plan Progress Charts -** The plan shall include appropriate progress/Gantt charts that reflect the proposed schedule and all major milestones. A sample project plan shall be submitted using Microsoft Project.

4. System Documentation

a. Describe the documentation provided to facilitate database support after contract is completed.

5. Acceptance Test Plan

Include a general acceptance test plan used for other File Maker Pro support engagements. The plan shall be modified after contract completed and will include the number of people to be involved in testing. The plan should document the acceptance testing approach, resources and/or tools that may be used to validate the functions and features of the proposed database support tasks. Include an example test plan that is representative of the structure, content, and level of detail planned for this project.

6. Risk Management

Submit a risk assessment using the methodology published by the Project Management Institute or other comparable methodology. Include risk mitigation strategies as well as the resources the using agency may utilize to reduce risk.

7. On-Going Service and Support

a. Describe the support activities that will be provided by the Offeror, specifically addressing the tasks outlined in the Invitation section.

b. Provide the normal hours and describe the channels (phone, email, web, etc.) for support. Describe how after hours support is provided. Describe the support and escalation process, including response times.

8. Value Added Services (Optional)

Offerors are encouraged but not required to propose any optional value added services they believe would help the using agency to effectively implement, operate or use the proposed system. Information provided in this section must be directly relevant to Filemaker Pro and not exceed two (2) pages in length.

APPENDIX B

PROPOSAL COST RESPONSE FORM

Offeror Name: _____

The Cost Proposal form will be provided via an addendum to the RFP after the Pre-Proposal Conference in August 24, 2010.

OFFEROR NAME: _____

APPENDIX C

NON-COLLUSION DECLARATION

I, _____, am the
(Print Name)
_____ of _____,
(Position/Title) (Name of Company)

the party making the foregoing proposal that the proposal is not made in the interest of, or on behalf of, any undisclosed person, partnership, company, association, organization, or corporation; that the bid is genuine and not collusive or sham; that the Offeror has not directly or indirectly induced or solicited any other Offeror to put in a false or sham bid; and has not directly or indirectly colluded, conspired, connived, or agreed with any Offeror or anyone else to put in a sham bid, or that anyone shall refrain from bidding; that the Offeror has not in any manner directly or indirectly, sought by agreement, communication, or conference with anyone to fix the bid price of the Offeror or any other Offeror, or to fix any overhead, profit, or cost element of the bid price, or of that of any other Offeror, or to secure any advantage against the public body awarding the contract of anyone interested in the proposed contract; that all statements contained in the bid are true; and, further, that the Offeror has not, directly or indirectly, submitted his or her bid price or any breakdown thereof, or the contents thereof, or divulged information or data relative thereto, or paid, and will not pay, any fee to any corporation, partnership, company association, organization, bid depository, or to any member or agent thereof to effectuate a collusive or sham bid.

I declare under penalty of perjury under the Laws of the State of California that the foregoing is true and correct:

COMPANY NAME: _____

AUTHORIZED
SIGNATURE _____

PRINT NAME: _____

DATE: _____

APPENDIX D

DECLARATION OF LOCAL BUSINESS

Santa Clara County gives local businesses a preference in formal solicitations of goods and services as set forth in the Board Policy, Section 5.3.13. A bidder or proposer has the option of qualifying for the preference by self-declaring its qualification as a "local business." By signing below, the bidder or proposer is certifying its qualification as a "local business" for purposes of application of Santa Clara County's policy and is deemed to be applying for the local preference.

All information submitted is subject to investigation, as well as to disclosure to third parties under the California Public Records Act. Incomplete, unclear, or incomprehensible responses to the following will result in the bid or proposal not being considered for application of Santa Clara County's local preference policy. False or dishonest responses will result in rejection of the bid or proposal and curtail the firm or individual's ability to conduct business with the County in the future. It may also result in legal action.

Provide the complete physical address of your business with meaningful "production capability" located within the boundary of the County of Santa Clara. The term "production capability" means sales, marketing, manufacturing, servicing, or research and development capability that substantially and directly enhances the firm's/bidder's/proposer's ability to perform the proposed contract. Post Office box numbers and/or residential addresses may not be used as the sole bases for establishing status as a "Local Business." If you have more than one physical address in Santa Clara County, please provide an attachment with all of the addresses in the form specified below.

Business Name:_____

Street: _____

City/State:_____ Zip Code:_____

Please Indicate Business Organization (Check One)

☐ Individual Proprietorship ☐ Corporation

☐ Partnership ☐ Other

By filling this form, bidder/proposer declares its qualification as a local business as defined in County of Santa Clara Board Policy, Section 5.3.13.

The undersigned declares that he or she is an official/agent of responding firm or individual and is empowered to represent, bind, and execute contracts on behalf of the firm or individual.

The undersigned declares under penalty of perjury, under the laws of the State of California, that all statements in this Exhibit and response are true and correct, with full knowledge that all statements are subject to investigation and that any incomplete, unclear, false or dishonest response may be grounds for denial or revocation of the accompanying bid or proposal and may result in being barred from doing business with Santa Clara County as well as additional legal consequences.

_____ _____
Signature Title

_____ _____
Name Date

_____
Business License Number (if applicable)

APPENDIX E

VENDOR REMOTE ACCESS AND USER RESPONSIBILITY

1. Scope of Access

a. "Remote Access" is the act of accessing County of Santa Clara ("County") systems from a non-County network infrastructure. "Systems" include personal computers, workstations, servers, mainframes, phone systems, and/or any device with network capabilities (e.g., a workstation with an attached modem, routers, switches, laptop computers, handheld devices).

b. County hereby grants Remote Access privileges for Contractor to access the following County systems, at the locations listed, collectively referred to as "IS," in accordance with the terms of the Agreement:

County Systems: _____

c. All other forms of access to the named Systems, or to any County System that is not specifically named, is prohibited.

d. Remote Access is granted for the purpose of Contractor providing services and performing its obligations as set forth in the Agreement including, but not limited to, supporting Contractor-installed programs. Any access to IS and/or County data or information that is not specifically authorized under the terms of this Agreement is prohibited and may result in contract termination and any penalty allowed by law.

e. County will review the scope of Contractor's Remote Access rights periodically. In no instance will Contractor's Remote Access rights be reduced, limited or modified in a way that prevents or delays Contractor from performing its obligations as set forth in the Agreement. Any modifications to Remote Access rights must be mutually agreed to in writing by County and Contractor.

2. Security Requirements

a. Contractor will not install any Remote Access capabilities on any County owned or managed system or network unless such installation and configuration is approved in writing by County's and Contractor's respective designees.

b. Contractor may only install and configure Remote Access capabilities on County systems or networks in accordance with industry standard protocols and procedures, which must be reviewed and approved by County's designee.

c. Contractor will only Remotely Access County systems, including access initiated from a County system, if the following conditions are met:

1. Contractor will submit documentation verifying its own network security mechanisms to County for County's review and approval. The County requires advanced written approval of Contractor's security mechanisms prior to Contractor being granted Remote Access.

2. Contractor Remote Access must include the following minimum control mechanisms:

a. Two-Factor Authentication: An authentication method that requires two of the following three factors to confirm the identity of the user attempting Remote Access. Those factors include: 1) something you possess (e.g., security token and/or smart card); 2) something you know (e.g., a personal identification number (PIN)); or 3) something you are (e.g., fingerprints, retina scan). The only exceptions are County approved County site to Contractor site Virtual Private Network (VPN) infrastructure.

b. Centrally controlled authorizations (permissions) that are user specific (e.g., access lists that limit access to specific systems or networks).

c. Audit tools that create detailed records/logs of access attempts.

d. All Contractor systems used to Remotely Access County systems must have industry-standard anti-virus and other security measures that might be required by the County (e.g., software firewall) installed, configured, and activated.

e. Access must be established through a centralized collection of hardware and software centrally managed and controlled by County's and Contractor's respective designees.

3. Monitoring/Audit

County will monitor access to, and activities on, County owned or managed systems and networks, including all Remote Access attempts. Data on all activities will be logged on a County managed system and will include the date, time, and user identification.

4. Copying, Deleting or Modifying Data

Contractor is prohibited from copying, modifying, or deleting any data contained in or on any County IS unless otherwise stated in the Agreement or unless Contractor receives prior written approval from County. This does not include data installed by the Contractor to fulfill its obligations as set forth in the Agreement.

5. Connections to Non-County Networks and/or Systems

Contractor agrees to make every effort to protect County's data contained on County owned and/or managed systems and networks within Contractor's control from unauthorized access. Prior written approval is required before Contractor may access County networks or systems from non-County owned and/or managed networks or systems. Such access will be made in accordance with industry standard protocols and procedures as mutually agreed upon and will be approved in writing by County in a timely manner. Remote Access must include the control mechanisms noted in Paragraph 2.c.2 above.

6. Person Authorized to Act on Behalf of Parties

The following persons are the designees for purposes of this Agreement:

Contractor: Title/ Designee _____

County: Title/ Designee _____

Either party may change the aforementioned names and or designees by providing the other party with no less than three (3) business days prior written notice.

7. Remote Access Provisions

Contractor agrees to the following:

a. Only staff providing services or fulfilling Contractor obligations under the Agreement will be given Remote Access rights.

b. Any access to IS and/or County information that is not specifically authorized under the terms of this Agreement is prohibited and may result in contract termination and any other penalty allowed by law.

c. An encryption method reviewed and approved by the County will be used. County is solely responsible and liable for any delay or failure of County, as applicable, to approve the encryption method to be used by Contractor where such delay or failure causes Contractor to fail to meet or perform, or be delayed in meeting or performing, any of its obligations under the Agreement.

d. Contractor will be required to log all access activity to the County. These logs will be kept for a minimum of 90 days and be made available to County no more frequently than once every 90 days.

8. Remote Access Methods

a. All forms of Remote Access will be made in accordance with mutually agreed upon industry standard protocols and procedures, which must be approved in writing by the County.

b. A Remote Access Back-Up Method may be used in the event that the primary method of Remote Access is inoperable.

c. Contractor agrees to abide by the following provisions related to the Primary and (if applicable) Backup Remote Access Methods selected below. (Please mark appropriate box for each applicable Remote Access Method; if a method is inapplicable, please check the box marked N/A).

1. VPN Site-to-Site ☐ **Primary** ☐ **Backup** ☐ **N/A**

The VPN Site-to-Site method involves a VPN concentrator at both the vendor site and at the County, with a secure “tunnel” opened between the two concentrators. If using the VPN Site-to-Site Method, Contractor support staff will have access to the designated software, devices and systems within the County, as specified above in Paragraph 1.b, from selected network-attached devices at the vendor site.

2. VPN Client Access ☐ **Primary** ☐ **Backup** ☐ **N/A**

In the VPN Client Access method, a VPN Client (software) is installed on one or more specific devices at the Contractor site, with Remote Access to the County (via a County VPN concentrator) granted from those specific devices only.

A CryptoCard will be issued to the Contractor in order to authenticate Contractor staff when accessing County IS via this method. The Contractor agrees to the following when issued a CryptoCard authentication device:

a. Because the CryptoCard allows access to privileged or confidential information residing on the County's IS, the Contractor agrees to treat the CryptoCard as it would a signature authorizing a financial commitment on the part of the Contractor.

b. The CryptoCard is a County-owned device, and will be labeled as such. The label must remain attached at all times.

c. The CryptoCard must be kept in a secured environment under the direct control of the Contractor, such as a locked office where public or other unauthorized access is not allowed.

d. If the Contractor's remote access equipment is moved to a non-secured site, such as a repair location, the CryptoCard will be kept under Contractor control.

e. The CryptoCard is issued to an individual employee of the Contractor and may only be used by the designated individual.

f. If the CryptoCard is misplaced, stolen, or damaged, the Contractor will notify County by phone within one (1) business day.

g. Contractor agrees to use the CryptoCard as part of its normal business operations and for legitimate business purposes only.

h. The CryptoCard will be issued to Contractor following execution of this Agreement. The CryptoCard will be returned to the County's designee within five (5) business days following contract termination, or upon written request of the County for any reason. Contractor will notify County's designee within one working day of any change in personnel affecting use and possession of the CryptoCard. Contractor will obtain the CryptoCard from any employee who no longer has a legitimate need to possess the CryptoCard. Lost or non-returned CryptoCards will be billed to the Contractor in the amount of $300 per card.

i. Contractor will not store password documentation or PINs with CryptoCards.

j. Contractor agrees that all employees, agents, contractors, and subcontractors who are issued the CryptoCard will be made aware of the responsibilities set forth in this Agreement in written form. Each person having possession of a CryptoCard will execute this Agreement where indicated below certifying that they have read and understood the terms of this Agreement.

3. County-Controlled VPN Client Access ☐ **Primary** ☐ **Backup** ☐ **N/A**

This form of Remote Access is similar to VPN Client access, except that the County will maintain control of the CryptoCard authentication token and a PIN number will be provided to the Contractor for use as identification for Remote Access purposes. When the Contractor needs to access County IS, the Contractor must first notify the County's designee.

The County's designee will verify the PIN number provided by the Contractor. After verification of the PIN the County's designee will give the Contractor a one-time password which will be used to authenticate Contractor when accessing the County's IS. Contractor agrees to the following:

a. Because the PIN number allows access to privileged or confidential information residing on the County's IS, the Contractor agrees to treat the PIN number as it would a signature authorizing a financial commitment on the part of the Contractor.

b. The PIN number is confidential, County-owned, and will be identified as such.

c. The PIN number must be kept in a secured environment under the direct control of the Contractor, such as a locked office where public or other unauthorized access is not allowed.

d. If the Contractor's remote access equipment is moved to a non-secured site, such as a repair location, the PIN number will be kept under Contractor control.

e. The PIN number can only be released to an authorized employee of the Contractor and may only be used by the designated individual.

f. If the PIN number is compromised or misused, the Contractor will notify the County's designee within one (1) business day.

g. Contractor will use the PIN number as part its normal business operations and for legitimate business purposes only. Any access to IS and/or County data information that is not specifically authorized under the terms of this Agreement is prohibited and may result in contract termination and any other penalty allowed by law.

h. The PIN number will be issued to Contractor following execution of this Agreement.

i. The PIN number will be inactivated by the County's designee within five (5) business days following contract termination, or as required by the County for any reason.

4. Manually Switched Dialup Modem ☐ **Primary** ☐ **Backup** ☐ **N/A**

Although not generally used, the Contractor may be provided Remote Access to County IS using a dialup modem. Contractor agrees to the following if using Switched Dialup Modem access:

a. Contractor will use reasonable efforts to notify the County's Technical Services Manager or designee at least ½ hour prior to access to allow County to activate the Switched Dialup Modem connection. Contractor

will give the estimated time that the connection will be required, and specify when the access can be deactivated by County.

b. County acknowledges that Contractor may not be able to provide certain of its services (including, but not limited to, implementation services, maintenance and support (including Standard Support Services) and training services) using a Switched Dialup Modem connection.

c. County is solely responsible and liable for any inability or delay in Contractor performing its obligations under the Agreement where such inability or delay is caused by the use of a Switched Dialup Modem connection.

Signatures of Contractor Employees receiving CryptoCards (if issued by County):

CONTRACTOR: _____

_____ [TYPE NAME HERE]

Date:_____

[TITLE]

CONTRACTOR: _____

_____ [TYPE NAME HERE]

Date:_____

[TITLE]

CONTRACTOR: _____

_____ [TYPE NAME HERE]

Date:_____

[TITLE]

INFORMATION TECHNOLOGY
USER RESPONSIBILITY STATEMENT AND INSTRUCTIONS

In May 1995 the Board of Supervisors charged each County organization with the responsibility for ensuring that all individuals within the organization had read and signed a statement of responsibility concerning use of the County's networks and information systems. This Statement is intended as a minimum Statement of User Responsibility, and individual County Agencies and Departments may make additions to strengthen it as necessary to meet any special requirements within their own environments.

- The User Responsibility Statement must be signed by everyone who might reasonably require access to a County network and/or information system, which includes County employees, consultants, contractors, sub-contractors, vendors, volunteers and any other authorized individual who is permitted access. All Users who are allowed to access County resources remotely must also sign an additional attachment specifically related to remote access; this is provided as Attachment C.
- Each County organization should identify a "User Responsibility Statement Administrator." This is an occasional personnel function that should NOT be filled by a member of the organization's Information System's support staff. A good choice would be a personnel administrator or office staff responsible for other routine personnel issues. The User Responsibility Statement Administrator is responsible for the following tasks:
    1. Identifying those employees, contractors and others within the organization that will need to read and sign the Statement.
    2. Managing the signing process, including arranging for any briefings that are held in conjunction with users signing the Statement.
    3. Maintaining the signed Statements.
    4. Documenting in the Agency / Departmental IT Security Plan that the Statements have been signed by all appropriate employees, contractors, and others.
    5. Ensuring that new employees, contractors, etc. read and sign the Statement.
- County organizations must identify all individuals who need to sign the Statement. For most organizations, the easiest approach would be to have everyone read and sign a Statement, but in some unusual cases it might make sense to exclude specific workgroups who clearly will never have the need to access a County computer or network.
- Following identification of the appropriate User communities, the Statements should be distributed for reading and signing. One possible method for accomplishing this is an all-staff briefing session, during which staff, contractors, etc. are presented with an overview of the Statement and then asked to sign it.
- It should be noted that individuals who sign the Statement are not required to agree with all of the Statement's provisions but that by signing they are acknowledging that they have read the Statement and understood its contents. The signer also acknowledges that violation of any of the Statement's provisions may result in disciplinary action and/or criminal prosecution.

- In rare situations where an individual refuses to sign the Statement the responsible Agency / Department may choose to read the Statement to the involved individual who will be required to verbally acknowledge understanding with two or more responsible managers present who will attest in writing that the reading and verbal attestation of understanding occurred. Failing a verbal acknowledgement of understanding the involved individual shall be denied access to all County information systems and networks.
- Each County organization is responsible for storing and maintaining all of the signed Statements. It is required that all County organizations have their users re-execute the Statement whenever there is an update or other change to the Statement. The Department Heads will be notified by the CIO's office of any updates or other changes to the Statement. It is recommended that all County organizations have their users re-execute the Statement annually. Also, all users that have remote access capabilities into the County must read and sign Attachment C of the Statement.

INFORMATION TECHNOLOGY USER RESPONSIBILITY STATEMENT

This User Responsibility Statement establishes a uniform, County-wide set of minimum responsibilities associated with being granted access to County information systems and/or County networks.

Definitions

County information systems and networks include all County-owned, rented, or leased desktop computers, laptop computers, handheld devices (including smart phones, wireless PDA's and Pocket PC's), equipment, networks, application systems, data bases and software; these items are typically under the direct control and management of County information system staff. Also included are information systems and networks under control and management of a service provider for use by the County.

Users includes full-time and part-time employees who are on the permanent County payroll, as well as other authorized individuals such as contractors, sub-contractors, consultants, temporary personnel, unpaid volunteers and any other authorized individual permitted access to County information systems and/or networks.

County-owned information/data is any information or data that is transported across a County network, or that resides in a County-owned information system, or on a network or system under control and management of a service provider for use by the County. This information/data is the exclusive property of the County of Santa Clara, unless excepted through constitutional provision, State or Federal statute, case law, or contract.

A *public record* is any writing, including electronic documents, relating to the conduct of the people's business.

1. General Code of Responsibility

The following General Code of Responsibility defines the basic standards for user interaction with County information systems and networks. All Users of County information systems and networks are required to comply with these standards.

1.1 Users are personally responsible for knowing and understanding the appropriate standards for User conduct, and are personally responsible for any actions they take that do not comply with County policies and standards.

1.2 Users must comply with County standards for password definition, use, and management. If a User is unclear as to the appropriate standards, it is the responsibility of the User to ask for guidance from their information systems support staff or Agency / Department management.

1.3 Users may not install, configure, or use any modem, any connection to a non-County network or system, or any wireless device, on any County system or network unless authorized to do so in writing by their designated departmental information systems support staff. If authorized to install, configure or use such a device or capability, Users must comply with all additional, applicable County standards designed to ensure the privacy and protection of data.

1.4 All connections between County information systems/networks and non-County systems/networks, including the Internet, must be approved by the County Chief Information Officer (CIO), or designee, and by the head of the involved Agency/Department. Users, including members of the County's information system

support staff, are prohibited from implementing such connections without obtaining this approval in writing.

1.5 No personally owned desktop computer, laptop computer, handheld and/or wireless device, or any other device may be attached to a County network unless such attachment is authorized in writing by designated departmental information systems support staff.

1.6 Users must not attempt to circumvent legal guidelines on software use and licensing by copying software. If a User is unclear as to whether a piece of software may be legitimately copied, it is the responsibility of the User to check with designated departmental information systems support staff.

1.7 Users may not install software on any County system unless specifically authorized to do so in writing by designated departmental information systems support staff.

1.8 Users are asked to be aware of security issues, and are encouraged to report incidents of security breaches (e.g., installation of an unauthorized device) to designated information systems support staff.

1.9 Users must understand and respect the sensitivity, privacy and confidentiality aspects of all County-owned information. In particular:

- Users must not attempt to access County systems or information unless authorized to do so, and there is a legitimate business need for such access.
- Users must not disclose information to anyone who does not have a legitimate need for that information.
- Users must not make or store printed or media-based (e.g., CD or floppy disk) copies of information unless it is a necessary part of that user's job.

1.10 Users must understand and respect the importance of County-owned data as a valuable asset. In particular:

- Users must not change or delete data or information unless performing such changes or deletions is a legitimate part of the user's job function.
- Users must avoid actions that might introduce malicious software, such as viruses or worms, onto any County system or network.

1.11 Users should be aware that electronic information transported across any County network, or residing in any County information system, is potentially subject to access by technical support staff, other County Users, and the general public. There are within the County IT environment systems and networks that have been made secure and private but in the absence of such special measures Users should not presume any level of data privacy for information transmitted over a County network, or stored within a County information system.

1.12 In general, Users must not use County systems or networks for personal activities that cannot be shown to either facilitate work tasks or increase job productivity. However, reasonable incidental (deminimus) personal use of County IT resources, such as Internet access and email, is allowed as long as such use does not interfere with the performance of work duties or the operation of the County's information systems. If a User is unclear as to appropriate personal uses, it is the responsibility of the User to ask for guidance from their Agency / Department management.

1.13 All information resources on any County information system or network are the property of the County and are therefore subject to County policies regarding acceptable use. No employee or other authorized User may use any County owned network, computer system, handheld and/or wireless device, cell phone or any other device or data for the following purposes:

- Personal profit, including commercial solicitation or conducting or pursuing their own business interested or those of another organization.
- Unlawful or illegal activities, including the downloading of licensed material without authorization, or downloading copyrighted material from the Internet without the publisher's permission.
- To access, create, transmit, print, download or solicit material that is or may be construed to be harassing or demeaning toward any individual or group for any reason, including on the basis of sex, age, race, color, national origin, creed, disability, political beliefs, organizational affiliation, or sexual orientation.
- To access, create, transmit, print, download or solicit sexually-oriented messages or images.
- The knowing propagation or downloading of viruses or other contaminants.
- The dissemination of hoaxes, chain letters, or advertisements.

1.14 Users that are employed by, or otherwise belong to, a HIPAA impacted Agency / Department are responsible for understanding and carrying out their responsibilities and duties as identified in the County HIPAA policies and procedures training.

1.15 Users should refer to the County's email retention policy for guidance with respect to the retention of email messages.

1.16 Users may not configure, access, use, or participate in those Internet services that have been prohibited by County policy, including but not limited to Internet Instant Messaging services (such as AOL Instant Messaging), Internet email services (such as hotmail), and peer-to-peer networking services (such as Kazaa), unless specifically authorized to do so in writing. All use of such services, even at a Departmental level, is subject to written approval and authorization procedures by the Department Head and the County CIO.

1.17 Users shall not use an internal County email account assigned to another individual to either send or receive emails.

1.18 Users shall not configure their email account to automatically forward email messages to an Internet or other external email system unless specifically authorized to do so in writing by their Department Head and the County CIO. Email messages that are manually forwarded must not contain information that is classified as confidential or restricted.

Acknowledgement of Receipt

This statement hereby incorporates Attachment A - Board of Supervisors Approved policy on "E-Mail", Attachment B – Board of Supervisors Approved Policy on "Internet Usage" and Attachment C - Additional Responsibilities for Users Accessing County IT Assets from a Non-County (Remote) Locations. Attachment C only applies to individuals that have been granted remote access privileges and should only be signed by those specific individuals. By signing this Statement, the following individual signifies that the County's User Responsibility Statement has been read and its contents understood. The signer also acknowledges that violation of any of its provisions may result in disciplinary action, leading up to and including termination and/or criminal prosecution.

The signer also acknowledges that this Statement will still be in effect following any transfer to another County Agency or Department, and that all of its provisions will continue to apply to the undersigned.

User Signature _____

Print User Name _____

Agency/Department _____

Date Signed _____

ATTACHMENT A - BOARD OF SUPERVISOR'S APPROVED POLICY

ON "E-MAIL"

Purpose of Policy

This policy addresses access to and the disclosure of information created, transmitted, received and stored via the County's e-mail systems. Access to e-mail is provided to employees and occasionally to other persons such as authorized contractors or volunteers (collectively referred to as "employees" in this policy), to assist them to perform their work, and their use of email must not jeopardize operation of the County's information systems or the reputation and integrity of the County. This policy is intended to ensure that County employees know their rights and responsibilities in using e-mail, and to ensure the appropriate, cost effective, and efficient use of County e-mail systems.

Use of the County's information systems must withstand public scrutiny. The California Public Records Act (CPRA), Government Code Section 6250, et. seq., requires the County to make all public records available for inspection and to provide copies upon request. A public record is any writing, including electronic documents, relating to the conduct of the people's business. Any information sent via e-mail may be subject to disclosure under the CPRA or requested in the process of litigation discovery. In addition, no use of licensed or copyrighted material should be made without permission from the holder of the license or copyright.

Appropriate Use of E-Mail

E-mail is provided as a business tool, however, its reasonable, incidental use for personal purposes is acceptable, so long as such use does not interfere with performance of work duties nor with the operation of the County's information systems.

A. No employee may use e-mail for inappropriate purposes, such as, but not limited to the following:

(1) Personal profit, including commercial solicitation or conducting or pursuing their own business interests or those of another organization.

(2) Unlawful or illegal activities.

(3) Creation or dissemination of harassing or demeaning statements toward any individual or group for any reason, including on the basis of sex, age, race, color, national origin, creed, disability, political beliefs, organizational affiliation, or sexual orientation.

(4) The dissemination of hoaxes, chain letters, or advertisements.

(5) The knowing propagation or downloading of viruses or other contaminants.

B. Employees should not create, send, forward, or reply to distribution lists concerning non-County business. Employees should consider the impact on the County's networks when creating and using large, work-related distribution lists.

Access to Messages

A. Employees should have no expectation of privacy in any messages sent via e-mail over the County's networks; employees should not use the system for any messages that they wish to remain private. Any electronic information transported across the County's networks is potentially subject to access by technical support staff, and review, monitoring, and disclosure by an audit authority designated by an employee's department head (or by the County Executive with respect to usage by department and agency

heads). All computer applications, programs, and work-related information created or stored by employees on the County's information systems are County property. If employees make incidental use of the e-mail system to transmit personal messages, such messages will be treated no differently from other messages.

B. The use of employee passwords and other message protection measures, other than those specifically authorized by the County, are prohibited. The County's authorization to use a password or other data protection measure shall not constitute consent by the County to maintain the messages as private.

C. This policy does not supplant the legal protections available to shield confidential, internal County communications from third party requests, such as information exempt from disclosure under the CPRA, shielded by attorney-client privilege, or subject to state law mandating confidentiality for specific subject matter.

Retention Policy

E-mail that is not necessary to the ordinary course of business should be routinely deleted.

Enforcement

Any violation of the County's e-mail policy may result in appropriate disciplinary action up to and including termination. Any improper e-mail will not be disclosed by the County to others except to the extent necessary to consider and to implement discipline, for other employment related purposes, or to respond to litigation requests. Potential criminal conduct which is revealed by improper e-mail will be referred to the appropriate law enforcement authorities.

ATTACHMENT B – BOARD OF SUPERVISOR'S APPROVED POLICY ON "INTERNET USAGE"

Purpose of Policy

The Internet has become an increasingly important source of information for County employees. Many County employees, and occasionally others such as contractors and volunteers (collectively referred to in this policy as "employees"), are provided access to the Internet to assist in the performance of their work for the County. However, the diversity of information available on the Internet brings with it the potential for abuse. This policy is intended to ensure that County employees know their rights and responsibilities in using the Internet, and to ensure the appropriate, cost effective, and efficient use of County Internet access capabilities.

Use of the Internet via the County's system must withstand public scrutiny. The California Public Records Act (CPRA), Government Code Section 6250, et. seq., requires the County to make all public records available for inspection and to provide copies upon request. A public record is any writing, including electronic documents, relating to the conduct of the people's business. The CPRA applies to information processed, sent and stored on the Internet. Additionally, records of Internet use may be requested during litigation discovery. No use of licensed or copyrighted material should be made without permission from the holder of the license or copyright.

Appropriate Internet Use

Access to the Internet is provided as a business tool, however, its reasonable, incidental use for personal purposes is acceptable, so long as such use does not interfere with performance of work duties or the operation of County information systems.

A. No employee, however, may use the Internet for inappropriate purposes, such as, but not limited to the following:

(1) Personal profit, including commercial solicitation or conducting or pursuing their own business interests or those of another organization.
(2) Unlawful or illegal activities, including the downloading of licensed material without authorization, or downloading copyrighted material from the Internet without the publisher's permission.
(3) To access, create, transmit, print, download or solicit material that is or may be construed to be harassing or demeaning toward any individual or group for any reason, including on the basis of sex, age, race, color, national origin, creed, disability, political beliefs, organizational affiliation, or sexual orientation.
(4) To access, create, transmit, print, download or solicit sexually-oriented messages or images.
(5) The knowing propagation or downloading of viruses or other contaminants.

B. Internet Relay Chat channels or other Internet forums such as newsgroups or net servers may be used only to conduct work-related business.

Access to Usage Records

A. Employees should have no expectation of privacy in their usage of the Internet. An audit authority designated by a department head may monitor usage of the Internet by department employees, including reviewing a list of sites accessed by an employee within the department; audit and examination of usage by an agency or department head shall be performed by a person designated by the County Executive. For this purpose, records of access to sites, materials and services on the Internet may be recorded and retained for a time period set by the County. The County or department head may restrict access to certain sites that it deems are not necessary for business purposes.

B. This policy does not supplant the legal protections available to shield confidential, internal County communications from third party requests, such as information exempt from disclosure under the CPRA, shielded by attorney-client privilege, or subject to state law mandating confidentiality for specific subject matter.

Enforcement

Violation of the County's policy on Internet use may result in appropriate disciplinary action up to and including termination. Any improper Internet usage will not be disclosed by the County to others except to the extent necessary to consider and to implement discipline, for other employment related purposes, or to respond to litigation requests. Potential criminal conduct which is revealed by inappropriate Internet usage will be referred to the appropriate law enforcement authorities.

Attachment C – Additional Responsibilities for Users Accessing County IT Assets from a Non-County (Remote) Locations

"*Remote access*" involves access to County Information Technology (IT) assets from a non-County infrastructure, no matter what technology is used to accomplish such access. This includes (but is not limited to) access to County IT assets from employee homes using modem-based or Internet connectivity, such as DSL or cable modem access. Systems that might be employed to accomplish such access include, but are not limited to, personal computers, workstations, laptops, palm-tops, "smart" phones, and any device that has network capabilities, such as routers and switches.

All remote access to County IT assets must be via secure, centralized, County-controlled mechanisms and technologies that have been reviewed and approved by the County CIO or designee. Users are not permitted to implement, configure, or use any remote access mechanism other than those that have been formally reviewed and approved in this manner. These approved technologies must include the following security features:

- Two-Factor Authentication: A strong method of authentication that verifies that the User is in fact the individual he is claiming to be. The two-factor authentication approach requires that the User provide two of the following three items: 1) something that the user has (such as a token card access device), 2) something that the user knows (such as a password or Personal Identification Number (PIN)), and 3) something that the user "is" (such as a fingerprint or retina scan). An equal or stronger authentication method may be used if approved by the County CIO or designee.
- User-specific, centrally controlled authorization (permissions) that limit User privileges once the User has been authenticated.
- Audit tools that create detailed records of all remote access attempts and remote access sessions including user identifier, date and time of access attempt.

The following regulations, responsibilities, and limitations apply to all Users attempting remote access to County IT assets, where a "User" is defined as "*any individual accessing and/or using County IT assets, including employees, contractors, sub-contractor, consultants, part-time employees, volunteers, and any other authorized individual attempting access or use of the County's IT infrastructure.*"

- Remote access is supported and provided only for those Users that have both read and signed the County's general User Responsibility Statement.
- Approval for use of County remote access mechanisms will be granted to a specific User, by the appropriate Agency/Department Head or designee, only on an individual, case-by-case basis. In general, approval for remote access is given only to those Users that require such access in order to perform their job functions.
- Remote access sessions may be monitored, recorded, and complete information on the session logged and archived. Users have no right, or expectation, of privacy when accessing County IT networks, systems, or data.

- Remote devices used for accessing County networks or systems may never be simultaneously connected to a non-County network or system, either directly or indirectly, while being used for remote access to the County, unless such a network or system is part of a remote access infrastructure approved by the County CIO or designee.
- All devices used to remotely access County IT assets must be configured according to County-approved security standards. These include installed, active, and current anti-virus software; software or hardware-based firewall; and any other security software or security-related system configurations that have been required and approved by the County.
- Users that have been provided with County-owned devices intended for remote access use, such as laptops and other portable devices, will take all reasonable care to ensure that these devices are protected from damage, access by third parties, loss, or theft.
- Remote access Users will practice due diligence in protecting the integrity of County networks, systems, and data while remotely accessing County IT assets. Specifically, all remote access sessions are subject to all other relevant County IT security policies and standards, including Local User Authentication, Data Classification, Internet Use, and Email.

Signature of Receipt:

By signing this statement, the User signifies that the contents of this Statement have been reviewed and understood, and that violation of its provisions may result in disciplinary action, leading up to and including termination and/or criminal prosecution.

The signer also acknowledges that this Statement will still be in effect following any transfer to another County Agency or Department, and that all of its provisions will continue to apply to the undersigned.

Agency: _____

Signature: _____ Date Signed: _____

APPENDIX F

PROPOSER'S TERMS AND CONDITIONS

Should an Offeror object to any of the County's terms and conditions in Attachment A, Offeror must propose specific alternative language and indicate the reason for the objection. The County may or may not accept the alternative language. General references to the Offeror's terms and conditions or attempts at complete substitutions are not acceptable to the County. Offerors must provide a brief discussion of the purpose and impact, if any, of each proposed changed followed by the specific proposed alternate wording.

In addition, Offerors must submit with their proposal any additional terms and conditions that they expect to have included in the contract negotiated with the County. Offerors must provide specific proposed wording and a brief discussion of the purpose and impact, if any. Include any applicable agreement, such as license, service level, maintenance, etc.

ATTACHMENT A

SAMPLE AGREEMENT TERMS AND CONDITIONS

The sample agreement will be posted as an addendum to the RFP after the Pre-Proposal Conference.

ATTACHMENT B
INSURANCE REQUIREMENTS FOR STANDARD SERVICE CONTRACTS
BETWEEN $50,001 AND $100,000

Indemnity

The Contractor shall indemnify, defend, and hold harmless the County of Santa Clara (hereinafter "County"), its officers, agents and employees from any claim, liability, loss, injury or damage arising out of or in connection with, performance of this Agreement by Contractor and/or its agents, employees or sub-contractors, excepting only loss, injury or damage caused by the negligence or willful misconduct of personnel employed by the County. It is the intent of the parties to this Agreement to provide the broadest possible coverage for the County. The Contractor shall reimburse the County for all costs, attorneys' fees, expenses and liabilities incurred with respect to any litigation in which the Contractor is obligated to indemnify, defend and hold harmless the County under this Agreement.

Insurance

Without limiting the Contractor's indemnification of the County, the Contractor shall provide and maintain at its own expense, during the term of this Agreement, or as may be further required herein, the following insurance coverages and provisions:

A. Evidence of Coverage

Prior to commencement of this Agreement, the Contractor shall provide a Certificate of Insurance certifying that coverage as required herein has been obtained. Individual endorsements executed by the insurance carrier shall accompany the certificate. In addition, a certified copy of the policy or policies shall be provided by the Contractor upon request.

This verification of coverage shall be sent to the requesting County department, unless otherwise directed. The Contractor shall not receive a Notice to Proceed with the work under the Agreement until it has obtained all insurance required and such insurance has been approved by the County. This approval of insurance shall neither relieve nor decrease the liability of the Contractor.

B. qualifying Insurers

All coverages, except surety, shall be issued by companies which hold a current policyholder's alphabetic and financial site category rating of not less than A- V, according to the current Best's Key Rating Guide or a company of equal financial stability that is approved by the County's Insurance Manager.

C. Notice of Cancellation

All coverage as required herein shall not be canceled or changed so as to no longer meet

the specified County insurance requirements without 30 days' prior written notice of such cancellation or change being delivered to the County of Santa Clara or their designated agent.

D. Insurance Required

1. Commercial General Liability Insurance - for bodily injury (including death) and property damage which provides limits as follows:

   a. Each occurrence - $1,000,000

   b. General aggregate - $1,000,000

   c. Products/Completed Operations aggregate - $1 ,000,000

   d. Personal Injury - $1,000,000

2. General liability coverage shall include:
   a.Premises and Operations
   b.Products/Completed
   c.Personal Injury liability
   d.Severability of interest

3. General liability coverage shall include the following endorsement, a copy of which shall be provided to the County:

   Additional Insured Endorsement, which shall read:

   > "County of Santa Clara, and members of the Board of Supervisors of the County of Santa Clara, and the officers, agents, and employees of the County of Santa Clara, individually and collectively, as additional insureds."

   Insurance afforded by the additional insured endorsement shall apply as primary insurance, and other insurance maintained by the County of Santa Clara, its officers, agents, and employees shall be excess only and not contributing with insurance provided under this policy. Public Entities may also be added to the additional insured endorsement as applicable and the contractor shall be notified by the contracting department of these requirements.

4. Automobile Liability Insurance

   For bodily injury (including death) and property, damage which provides total limits of not less than one hundred thousand dollars ($100,000) combined single limit per occurrence applicable to all owned, non-owned and hired vehicles.

4a. Aircraft/Watercraft Liability Insurance (Required if Contractor or any of its agents or subcontractors will operate aircraft or watercraft in the scope of the Agreement)

For bodily' injury (including death) and property damage which provides total limits of not less than one hundred thousand dollars ($100,000) combined single limit per occurrence applicable to all owned, non-owned and hired aircraft/watercraft.

5. Workers' Compensation and Employer's Liability Insurance

a. Statutory California Workers' Compensation coverage including broad form all-states coverage.

b. Employer's Liability coverage for not less than one million dollars ($1,000,000) per occurrence.

F. Special Provisions

The following provisions shall apply to this Agreement:

The foregoing requirements as to the types and limits of insurance coverage to be maintained by the Contractor and any' approval of said insurance by the County or its insurance consultant(s) are not intended to and shall not in any manner limit or qualify the liabilities and obligations otherwise assumed by the Contractor pursuant to this Agreement, including but not limited to the provisions concerning indemnification.

2. The County' acknowledges that some insurance requirements contained in this Agreement may be fulfilled by self-insurance on the part of the Contractor. However, this shall not in any way limit liabilities assumed by the Contractor under this Agreement. Any self-insurance shall be approved in writing by the County upon satisfactory evidence of financial capacity. Contractors obligation hereunder may be satisfied in whole or in part by adequately' funded self-insurance programs or self-insurance retentions.

3. Should any of the work under this Agreement be sublet, the Contractor shall require each of its subcontractors of any tier to carry the aforementioned coverages, or Contractor may insure subcontractors under its own policies.

4. The County reserves the right to withhold payments to the Contractor in the event of material noncompliance with the insurance requirements outlined above.

F. Fidelity Bonds (Required only if contractor will be receiving advanced funds or payments)

Before receiving compensation under this Agreement, Contractor will furnish County with evidence that all officials, employees, and agents handling or having access to funds received or disbursed under this Agreement, or authorized to sign or countersign checks, are covered by a BLANKET FIDELITY BOND in an amount of AT LFAST fifteen percent *(15%)* of the maximum financial obligation of the County cited herein. If such bond is canceled or reduced, Contractor will notify County immediately, and County may' withhold further payment to Contractor until proper coverage has been obtained. Failure to give such notice may be cause for termination of this Agreement, at the option of County.

ATTACHMENT C
BUSINESS ASSOCIATE AGREEMENT

WHEREAS, County of Santa Clara ("County" or "Covered Entity") is a Covered Entity, as defined below, and wishes to disclose certain Protected Health Information ("PHI") to _____ "Business Associate" pursuant to the terms of the Agreement and this amendment ("Business Associate Agreement" or "BAA"); and

WHEREAS, Covered Entity and Business Associate intend to protect the privacy and provide for the security of PHI disclosed to Business Associate pursuant to the Contract in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("the HITECH Act"), and regulations promulgated thereunder by the U.S. Department of Health and Human Services (the "HIPAA Regulations") and other applicable law; and

WHEREAS, as part of the HIPAA Regulations, the Privacy Rule and the Security Rule (defined below) require Covered Entity to enter into a contract containing specific requirements with Business Associate prior to the disclosure of PHI, as set forth in, but not limited to, Title 45, Sections 164.314(a), 164.502(e) and 164.504(e) of the Code of Federal Regulations ("C.F.R.") and contained in this Addendum.

In consideration of the mutual promises below and the exchange of information pursuant to this Addendum, the parties agree as follows:

I. Definitions

Terms used, but not otherwise defined, and terms with initial capital letters in this provision of the Agreement have the same meaning as defined under the Health Insurance Portability and Accountability Act of 1996, 42 USC §§ 1320d et seq. ("HIPAA") and the implementing regulations and with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("the HITECH Act"), and regulations promulgated thereunder by the U.S. Department of Health and Human Services (the "HIPAA Regulations") and other applicable laws.

Privacy Breach: Any reported, suspected, actual or alleged acquisition, access, use or disclosure of Protected Health Information in a manner not permitted or allowed under state or federal privacy laws.

Business Associate – A person, organization, or agency other than a workforce member that provides specific functions, activities, or services that involve the use, creation, or disclosure of PHI for, or on behalf of, a HIPAA covered health care component. Examples of business associate functions are activities such as claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, practice management, and repricing; and legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

Covered Entity shall have the meaning given to such term under the Privacy Rule and the Security Rule, including, but not limited to, 45 C.F.R. Section 160.103.

Designated Record Set shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.

Electronic Protected Health Information means Protected Health Information that is maintained in or transmitted by electronic media.

Electronic Health Record shall have the meaning given to such term in the HITECT Act, including, but not limited to, 42 U.S.C. Section 17921.

Health Care Operations shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.

Privacy Rule shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and E.

Protected Health Information or PHI means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501. Protected Health Information includes Electronic Protected Health Information [45 C.F.R. Sections 160.103, 164.501].

Protected Information shall mean PHI provided by Santa Clara County to Business Associate or created or received by Business Associate on Santa Clara County's behalf.

Security Rule shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and C.

Unsecured PHI shall have the meaning given to such term under the HITECH Act and any guidance issued pursuant to such Act including, but not limited to, 42 U.S.C. Section 17932(h).

II. Duties & Responsibilities of Business Associate

a. Permitted Uses. Business Associate shall not use Protected Information except for the purpose of performing Business Associate's obligations under the Contract and as permitted under the Contract and Addendum. Further, Business Associate shall not use Protected Information in any manner that would constitute a violation of the Privacy Rule or the HITECH Act if so used by CE. However, Business Associate may use Protected Information (i) for the proper management and administration of Business Associate, (ii) to carry out the legal responsibilities of Business Associate, or (iii) for Data Aggregation purposes for the Health Care Operations of CE [45 C.F.R. Sections 164.504(e)(2)(ii)(A) and 164.504(e)(4)(i)].

b. Permitted Disclosures. Business Associate shall not disclose Protected Information except for the purpose of performing Business Associate's obligations under the Contract and as permitted under the Contract and Addendum. Business Associate shall not disclose Protected Information in any manner that would constitute a violation of the Privacy Rule or the HITECH Act if so disclosed by CE. However, Business Associate may disclose Protected Information (i) for the proper management and administration of Business Associate; (ii) to carry out the legal responsibilities of Business Associate; (iii) as required by law; or (iv) for Data Aggregation purposes for the Health Care Operations of CE. If Business Associate discloses Protected Information to a third party, Business Associate must obtain, prior to making any such disclosure, (i) reasonable written assurances from such third party that such Protected Information will be held confidential as provided pursuant to this Addendum and only disclosed as required by law or for the purposes for which is was disclosed to such third party, and (ii) a written agreement from such third party to immediately notify Business Associate of any breaches of confidentiality of the Protected Information within 10 calendar days of discovery, to the extent it has obtained knowledge of such breach [42 U.S.C. Section 17932; 45 C.F.R. Sections 164.504(e)(2)(i), 164.504(e)(2)(i)(B), 164.504(e)(2)(ii)(A) and 164.504(e)(4)(ii)].

c. Prohibited Uses and Disclosures. Business Associate shall not use or disclose Protected Information for fundraising or marketing purposes. Business Associate shall not disclose Protected Information to a health plan for payment or health care operations purposes if the patient has requested this special restriction, and has paid out of pocket in full for the health care item or service to which the PHI solely relates [42 U.S.C. Section 17935(a)]. Business Associate shall not directly or indirectly receive remuneration in exchange for Protected Information, except with the prior written consent of CE and as permitted by the HITECH Act, 42 U.S.C. section 17935(d)(2); however, this prohibition shall not affect payment by CE to Business Associate for services provided pursuant to the Contract.

d. Appropriate Safeguards. Business Associate Shall implement appropriate safeguards as are necessary to prevent the use or disclosure of Protected Information otherwise than as permitted by the Contract that reasonably and appropriately protect the confidentiality, integrity and availability of the Protected Information,

in accordance with 45 C.F.R. Sections 164.308, 164.310, 164.312 and 164.316. [45 C.F.R. Section 164.504(e)(2)(ii)(B); 45 C.F.R. Section 164.308(b)]. Business Associate shall comply with the policies and procedures and documentation requirements of the HIPAA Security Rule, including, but not limited to, 45 C.F.R. Section 164.316 [42 U.S.C. Section 17931].

e. Reporting of Improper Access, Use or Disclosure. Business Associate shall report to CE in writing of any access, use or disclosure of Protected Information not permitted by the Contract and Addendum, and any Breach of Unsecured PHI of which it becomes aware without unreasonable delay and in no case later than 10 calendar days after discovery [42 U.S.C. Section 17921; 45 C.F.R. Section 164.504(e)(2)(ii)(C); 45 C.F.R. Section 164.308(b)]. The breach notice must contain: (1) a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known, (2) a description of the types of PHI that were involved in the breach, (3) any steps individuals should take to protect themselves from potential harm resulting from the breach, (4) a brief description of what the business associate is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches, and (5) contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website or postal address. [45 C.F.R Section 164.410] Business Associate shall take (i) prompt corrective action to cure any such deficiencies and (ii) any action pertaining to such unauthorized disclosure required by applicable federal and state laws and regulations.

f. Business Associate's Agents. Business Associate shall ensure that any agents, including subcontractors, to whom it provides Protected Information, agree in writing to the same restrictions and conditions that apply to Business Associate with respect to such PHI and implement the safeguards required by paragraph c above with respect to Electronic PHI [45 C.F.R. Section 164.504(e)(2)(ii)(D); 45 C.F.R. Section 164.308(b)]. Business Associate shall implement and maintain sanctions against agents and subcontractors that violate such restrictions and conditions and shall mitigate the effects of any such violation (see 45 C.F.R. Sections 164.530(f) and 164.530(e)(1)).

g. Access to Protected Information. Business Associate shall make Protected Information maintained by Business Associate or its agents or subcontractors in Designated Record Sets available to CE for inspection and copying within ten (10) days of a request by CE to enable CE to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.524 [45 CF.R. Section 164.504(e)(2)(ii)(E)]. If Business Associate maintains an Electronic Health Record, Business Associate shall provide such information in electronic format to enable CE to fulfill its obligations under the HITECH Act, including, but not limited to, 42 U.S.C. Section 17935(e).

h. Electronic PHI. If Business Associate receives, creates, transmits or maintains EPHI on behalf of COVERED ENTITY, Business Associate will, in addition, do the following:

(1) Develop, implement, maintain and use appropriate administrative, physical, and technical safeguards in compliance with Section 1173(d) of the Social Security Act, Title 42, Section 1320(s) or the United States Code and Title 45, Part 162 and 164 of CFR to preserve the integrity and confidentiality of all electronically maintained or transmitted PHI received from or on behalf of COVERED ENTITY.

(2) Document and keep these security measures current and available for inspection by COVERED ENTITY.

(3) Ensure that any agent, including a subcontractor, to whom the Business Associate provides EPHI agrees to implement reasonable and appropriate safeguards to protect it.

(4) Report to the COVERED ENTITY any Security Incident of which it becomes aware. For the purposes of this Agreement, Security Incident means, as set forth in 45 C.F.R section 164.304, "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."

i. Amendment of PHI. Within ten (10) days of receipt of a request from Santa Clara County for an amendment of Protected Information or a record about an individual contained in a Designated Record Set, Business Associate or its agents or subcontractors shall make such Protected Information available to Santa Clara County for amendment and incorporate any such amendment to enable Santa Clara County to fulfill its obligations under the Privacy Rule. If any individual requests an amendment of Protected Information directly from Business

Associate or its agents or subcontractors, Business Associate must notify Santa Clara County in writing within five (5) days of the request. Any approval or denial of amendment of Protected Information maintained by Business Associate or its agents or subcontractors shall be the responsibility of CE.

j. Accounting Rights. Promptly upon any disclosure of Protected Information for which Santa Clara County is required to account to an individual, Business Associate and its agents or subcontractors shall make available to Santa Clara County the information required to provide an accounting of disclosures to enable Santa Clara County to fulfill its obligations under the Privacy Rule, and the HITECH Act, as determined by CE. Business Associate agrees to implement a process that allows for an accounting to be collected and maintained by Business Associate and its agents or subcontractors for at least six (6) years prior to the request. Accounting of disclosures from an Electronic Health Record for treatment, payment or health care operations purposes are required to be collected and maintained for three (3) years prior to the request, and only to the extent Business Associate maintains an electronic health record and is subject to this requirement.

At a minimum, the information collected and maintained shall include: (i) the date of disclosure; (ii) the name of the entity or person who received Protected Information and, if known, the address of the entity or person; (iii) a brief description of Protected Information disclosed and (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's authorization, or a copy of the written request for disclosure. In the event that the request for an accounting is delivered directly to Business Associate or its agents or subcontractors, Business Associate shall within five (5) days of a request forward it to Santa Clara County in writing. It shall be CE's responsibility to prepare and deliver any such accounting requested. Business Associate shall not disclose any Protected Information except as set forth in Agreement.

k. Governmental Access to Records. Business Associate shall make its internal practices, books and records relating to the use and disclosure of Protected Information available to Santa Clara County and to the Secretary of the U.S. Department of Health and Human Services (the "Secretary") for purposes of determining Business Associate s compliance with the Privacy Rule. Business Associate shall provide to Santa Clara County a copy of any Protected Information that Business Associate provides to the Secretary concurrently with providing such Protected Information to the Secretary.

l. Minimum Necessary. Business Associate (and its agents or subcontractors) shall request, use and disclose only the minimum amount of Protected Information necessary to accomplish the purpose of the request, use, or disclosure. Business Associate understands and agrees that the definition of "minimum necessary" is in flux and shall keep itself informed of guidance issued by the Secretary with respect to what constitutes "minimum necessary."

m. Data Ownership. Business Associate acknowledges that Business Associate has no ownership rights with respect to the Protected Information.

n. Breach Pattern or Practice by Covered Entity. If the Business Associate knows of a pattern of activity or practice of the Santa Clara County that constitutes a material breach or violation of the CE's obligations under the Contract or Addendum or other arrangement, the Business Associate must take reasonable steps to cure the breach or end the violation. If the steps are unsuccessful, the Business Associate must terminate the Contract or other arrangement if feasible, or if termination is not feasible, report the problem to the Secretary of DHHS. Business Associate shall provide written notice to Santa Clara County of any pattern of activity or practice of the Santa Clara County that Business Associate believes constitutes a material breach or violation of the CE's obligations under the Contract or Addendum or other arrangement within five (5) days of discovery and shall meet with Santa Clara County to discuss and attempt to resolve the problem as one of the reasonable steps to cure the breach or end the violation.

o. Audits, Inspection and Enforcement. Within ten (10) days of a written request by CE, Business Associate and its agents or subcontractors shall allow Santa Clara County to conduct a reasonable inspection of the facilities, systems, books, records, agreements, policies and procedures relating to the use or disclosure of Protected Information pursuant to this Addendum for the purpose of determining whether Business Associate has complied with this Addendum; provided, however, that (i) Business Associate and Santa Clara County

shall mutually agree in advance upon the scope, timing and location of such an inspection, (ii) Santa Clara County shall protect the confidentiality of all confidential and proprietary information of Business Associate to which Santa Clara County has access during the course of such inspection; and (iii) Santa Clara County shall execute a nondisclosure agreement, upon terms mutually agreed upon by the parties, if requested by Business Associate .

The fact that Santa Clara County inspects, or fails to inspect, or has the right to inspect, Business Associate 's facilities, systems, books, records, agreements, policies and procedures does not relieve Business Associate of its responsibility to comply with this Addendum, nor does CE's (i) failure to detect or (ii) detection, but failure to notify Business Associate or require Business Associate 's remediation of any unsatisfactory practices, constitute acceptance of such practice or a waiver of CE's enforcement rights under the Contract or Addendum, Business Associate shall notify Santa Clara County within ten (10) days of learning that Business Associate has become the subject of an audit, compliance review, or complaint investigation by the Office for Civil Rights.

III. Termination

a. Material Breach. A breach by Business Associate of any provision of this Addendum, as determined by CE, shall constitute a material breach of the Contract and shall provide grounds for immediate termination of the Contract, any provision in the Contract to the contrary notwithstanding [45 C.F.R. Section 164.504(e)(2)(iii)].

b. Judicial or Administrative Proceedings. Santa Clara County may terminate the Contract, effective immediately, if (i) Business Associate is named as a defendant in a criminal proceeding for a violation of HIPAA, the HITECH Act, the HIPAA Regulations or other security or privacy laws or (ii) a finding or stipulation that the Business Associate has violated any standard or requirement of HIPAA, the HITECH Act, the HIPAA Regulations or other security or privacy laws is made in any administrative or civil proceeding in which the party has been joined.

c. Effect of Termination. Upon termination of the Contract for any reason, Business Associate shall, at the option of CE, return or destroy all Protected Information that Business Associate or its agents or subcontractors still maintain in any form, and shall retain no copies of such Protected Information. If return or destruction is not feasible, as determined by CE, Business Associate shall continue to extend the protections of Section 2 of this Addendum to such information, and limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible. [45 C.F.R. Section 164.504(e)(ii)(2(I)]. If Santa Clara County elects destruction of the PHI, Business Associate shall certify in writing to Santa Clara County that such PHI has been destroyed.

IV. General Provisions

a. Indemnification. In addition to the indemnification language in the Agreement, Business Associate agrees to be responsible for, and defend, indemnify and hold harmless the County for any breach of Business Associate's privacy or security obligations under the Agreement, including any fines and assessments that may be made against SCVHHS or the Business Associate for any privacy breaches or late reporting.

b. Disclaimer. The County of Santa Clara makes no warranty or representation that compliance by Business Associate with this Addendum, HIPAA, the HITECH Act, or the HIPAA Regulations will be adequate or satisfactory for Business Associate's own purposes. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI.

c. Amendment to Comply with Law. The parties acknowledge that state and federal laws relating to data security and privacy are rapidly evolving and that amendment of the Contract of Addendum may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule and other applicable laws relating to the security or confidentiality of PHI. The parties understand and agree that Santa Clara County must receive satisfactory written assurance from Business Associate that Business Associate will adequately safeguard all Protected Information.

Upon the request of either party, the other party agrees to promptly enter into negotiations concerning the terms of an amendment to this Addendum embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule or other applicable laws. Santa Clara County may terminate the Contract upon thirty (30) days written notice in the event (i) Business Associate does not promptly enter into negotiations to amend the Contract or Addendum when requested by Santa Clara County pursuant to this Section or (ii) Business Associate does not enter not enter into an amendment to the Contract or Addendum providing assurances regarding the safeguarding of PHI that CE, in its sole discretion, deems sufficient to satisfy the standards and requirements of applicable laws.

d. Assistance in Litigation of Administrative Proceedings. Business Associate shall make itself, and any subcontractors, employees or agents assisting Business Associate in the performance of its obligations under the Contract or Addendum, available to CE, at no cost to CE, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CE, its directors, officers or employees based upon a claimed violation of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule, or other laws relating to security and privacy, except where Business Associate or its subcontractor, employee or agent is named adverse party.

e. No Third-Party Beneficiaries. Nothing express or implied in the Contract or Addendum is intended to confer, nor shall anything herein confer, upon any person other than CE, Business Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

f. Effect on Contract. Except as specifically required to implement the purposes of this Addendum, or to the extent inconsistent with this Addendum, all other terms of the Contract shall remain in force and effect.

g. Interpretation. The provisions of this Addendum shall prevail over any provisions in the Contract that may conflict or appear inconsistent with any provision in this Addendum. This Addendum and the Contract shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, the Privacy Rule and the Security Rule. The parties agree that any ambiguity in this Addendum shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act, the Privacy Rule and the Security Rule.

h. Survivorship. The respective rights and responsibilities of Business Associate related to the handling of PHI survive termination of this Agreement.

IN WITNESS WHEREOF, the parties hereto have duly executed this Addendum as of the Addendum Effective Date.

COVERED ENTITY
By: _____ Date _____
Print Name: _____
Title: _____ _____

BUSINESS ASSOCIATE
By: _____ Date _____
Print Name: _____
Title: _____ _____

Health Information Technology for Economic and Clinical Health Act (HITECH Act) Business Associate Requirements

These additional terms and conditions shall be incorporated into and made a part of the Payment Services Agreement ("Agreement") between the County of Santa Clara ("County") and _____("Contractor"). Exhibit H is incorporated into the Agreement. To the extent there are conflicts between the terms and conditions of Exhibit H and the Agreement, Exhibit H shall control.

The Health Information Technology for Economic and Clinical Health Act (HITECH Act), Pub. L. 111-5, Div. A, Title XIII, § 130001 et seq., Div. B, Title IV, § 4001 et seq., Feb. 17, 2009, 123 Stat. 226, 467, 42 U.S.C.A. § 300ii, et seq., and 42 U.S.C. A, § 17901, et seq., which was signed February 17, 2009 as part of the American Recovery and Reinvestment Act of 2009 (ARRA) requires that additional privacy and security requirements be incorporated into all business associate agreements with covered entities under the Health Insurance Portability and Accountability Act (HIPAA) effective February 17, 2010. (42 U.S.C. §§ 17931 and 17934).

The HITECH Act requires that certain provisions of the HIPAA Security Rule be incorporated into business associate agreements, including: (1) Administrative safeguards (45 C.F.R. Section 164.308); (2) Physical safeguards (45 C.F.R. section 164.310); (3) Technical safeguards (45 C.F.R. section 164.312); and (4) policies and procedures and documentation requirements (45 C.F.R. section 164.316); (5) compliance reviews and investigations; and (5) other additional privacy provisions contained in the HITECH Act. Business associates may be subject to the same civil and criminal penalties as are HIPAA covered entities. (42 U.S.C., 42 U.S.C. §§ 17931 and 17934).

The County is preparing a modified business associate agreement to reflect these new requirements, which will be available prior to February 17, 2010. Pursuant to the HITECH Act, Contractor shall enter into this modified agreement effective February 17, 2010.

Moreover, **effective September 23, 2009**, the HITECH Act requires Contractor to inform the County without unreasonable delay and no later than sixty (60) calendar days after discovery of a privacy breach, meaning a patient whose protected health information (PHI) has been (or is reasonably believed by the business associate to have been) accessed, acquired, or disclosed in a manner not permitted by HIPAA and federal privacy laws. (45 C.F.R., § 164.410.) The notice must contain: (1) a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known, (2) a description of the types of PHI that were involved in the breach, (3) any steps individuals should take to protect themselves from potential harm resulting from the breach, (4) a brief description of what the business associate is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches, and (5) contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address. (42 C.F.R. § 164.410).

When the County is notified of a breach of unsecured PHI by a business associate, or if the County has reason to know of a breach of unsecured PHI by a business associate, the County's

own sixty (60) day notification obligations (to the patient whose PHI was breached and to the Secretary of the Department of Health and Human Services) may be triggered.

In order to comply with the HITECH law and to ensure that all reporting obligations on the part of both the County and Contractor are timely met and satisfied, effective immediately, Contractor must notify the County Compliance and Privacy Officer without unreasonable delay and in any event no later than ten (10) business days following the discovery of any potential privacy breach. A breach is discovered by Contractor as of the first day on which such breach is known to Contractor, or, by exercising reasonable diligence, would have been known to the Contractor. Contractor shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence, would have been known to any person, other than the person committing the breach, who is an employee, officer, or other agent of the Contractor. The contact information for the Compliance and Privacy Officer is as follows:

Anna Hughes, MPA
Compliance & Privacy Officer
Santa Clara Valley Health & Hospital System
2325 Enborg Lane, Suite 360
San Jose, CA 95128
Telephone: 408-885-3794
E-mail: anna.hughes@hhs.sccgov.org
Fax: 408-885-6886

The notification to the County Compliance and Privacy Officer may be accomplished by telephone, fax or e-mail.

Contractor shall be responsible for, and defend, hold harmless and indemnify the County for any fines and assessments that may be imposed on the County, any SCVHHS entity or the Contractor for any privacy breaches or late reporting by Contractor.