THE INFORMATION IN THIS BOX IS NOT A PART OF THE CONTRACT AND IS FOR COUNTY USE ONLY

Contract Number

SAP Number

County Administrative Office

Department Contract Representative	Danette Tealer
Telephone Number	(909) 387-5420

Contractor	Plante & Moran, PLLC
Contractor Representative	Furney Brown
Telephone Number	(248) 223-3396
Contract Term	February 11, 2020-February 10, 2021
Original Contract Amount	$603,000
Amendment Amount	
Total Contract Amount	$603,000
Cost Center	Various

IT IS HEREBY AGREED AS FOLLOWS*:*

WHEREAS, the County of San Bernardino, hereafter referred to as "County," desires Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) Privacy and Security Risk Analysis services; and

WHEREAS, the County conducted a competitive process to find a contractor to provide such services; and

WHEREAS, Plante & Moran, PLLC, hereafter referred to as "Consultant," submitted a proposal and was determined qualified to provide these services, and

WHEREAS, the County desires that such services be provided by Consultant and Consultant agrees to perform these services as set forth below;

NOW, THEREFORE, the County and Consultant mutually agree to the following terms and conditions:

TABLE OF CONTENTS

I. DEFINITIONS

A. Board: The San Bernardino County Board of Supervisors.

B. Business Associate: A person or organization that on behalf of a covered entity, other than a member of the covered entity's workforce creates, receives, maintains, or transmits Protected Health Information (PHI).

C. Contract: The Contract between the County and the Proposer resulting from the award issued pursuant to this RFP to the successful Proposer.

D. Consultant: Any individual, company, firm, corporation, partnership or other organization to whom a contract award is made by the County.

E. Covered Entity: A health plan, health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a HIPAA covered transaction.

F. Electronic Protected Health Information (ePHI) – Protected Health Information maintained in electronic form.

G. Health Care Component (HCC): County departments or programs that meet the definition of a Covered Entity or Internal Business Associate as designated by County Policy 14-03 and Standard Practice 14-03SP01. The HCC includes the following departments and programs:

   a. Aging and Adult Services - Multipurpose Senior Services Program
   b. Arrowhead Regional Medical Center
   c. Auditor/Controller-Treasurer-Tax Collector – Central Collections)
   d. Behavioral Health
   e. Board of Supervisors
   f. County Administrative Office
   g. County Counsel
   h. Human Resources - Employee Benefits and Services Division
   i. Information Services
   j. Public Health
   k. Risk Management

H. Health Insurance Portability and Accountability Act: A federal law designed to provide privacy and information security standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals, and other health care providers. (45 CFR parts 160 and 164.)

I. Internal Business Associate: A County department or program that provides services to another County department or program covered by HIPAA that if it was a separate legal entity would fall within the definition of a Business Associate.

J. Mobile Device: A general term for any handheld device such as a smart phone, tablet, cell phone, laptop, wearables (e.g., smart watch), etc.

K. Protected Health Information (PHI): Individually identifiable health information that is transmitted by, or maintained in, electronic media or any other form or medium (excludes individually identifiable health information in employment records held by Covered Entity in its role as employer).

L. Risk: The likelihood that a threat will exploit a vulnerability, and the impact of that event on the confidentiality, availability, and integrity of ePHI, other confidential or proprietary electronic information, and other system assets.

M. Risk Analysis: An accurate and thorough assessment that:
- Identifies the risks to information system security and determines the probability of occurrence and the resulting impact for each threat/vulnerability pair identified given the security controls in place;
- Prioritizes risk; and
- Results in recommended possible actions/controls that could reduce or offset the determined risk.

Risk levels shall be modeled using Exhibit B to assist in prioritizing mitigation of those risks.

N. Risk Management: A process that prioritizes, evaluates, and implements security controls that will reduce or offset the risks determined in the risk analysis process to satisfactory levels within an organization given its mission and available resources.

O. Selected Sites: A site within the purview of an HCC department or program where services will be performed.

II. PURPOSE

Pursuant to 45 Code of Federal Regulations (CFR) section 164.105, the County has designated itself as a hybrid entity. The County is entering into this Agreement with Consultant to provide Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) Privacy and Security Risk Analysis services for departments identified as part of the hybrid entity through the designation of the County's Health Care Component (HCC). In an effort to ensure/achieve compliance with HIPAA/HITECH across all portions of the HCC, the County has endeavored to create minimum standards and practices for implementation countywide. In furtherance of that effort, the County desires to utilize this Agreement to complete a HIPAA/HITECH Security Risk Analysis that meets the requirements of 45 CFR section 164.308(a), for each HCC department and the County. Departments are responsible for determining which locations they desire to be included as part of their services.

In addition, at the option of each HCC department, a HIPAA Privacy Rule Gap Analysis and Physical Assessment may be requested. The selection of the additional analyses to be completed will be dependent upon the best interest of those departments. Not all departments will require the full range of services described in Section III – Consultant Responsibilities. Consultant must be flexible in working with individual departments to determine needs, budgetary constraints, and develop a specific scope of work.

III. CONSULTANT RESPONSIBILITIES

A. PROJECT DESCRIPTION

This Scope of Work (SOW) is to provide a Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) Privacy and Security Risk Analysis for multiple County of San Bernardino (County) Health Care Component (HCC) Departments and perform other services as further described below. **This SOW is structured in conformity with the categories described below, where Categories 1 and 2 are**

mandatory for all HCC Departments. Categories 3 and 4 are elective dependent upon HCC Department need. All sections referenced below are from Title 45 of the CFR.

Consultant shall work with each County's/HCC Department's designated representative to discuss and agree upon the specific timeframes and tools that will be used in providing services pursuant to this Agreement to minimize any potential impact to the HCC Department. Prior to engagement in assessment activities, Consultant shall receive approval from the designated representative for the HCC Department.

1. HIPAA Risk Analysis (45 CFR §164.308(a)(1)(ii)(A)) (Mandatory)

The HIPAA Risk Analysis must be conducted in accordance with the National Institute of Standards and Technology (NIST), and International Organization for Standardization (ISO) standards and consist of the following components for each HCC Department:

a. **Manual Testing.** Test the HCC Department's ability to prevent and/or identify an ongoing attack through a targeted attack simulation initiated from external network attack vectors (i.e., blind test) and from pre-determined internal network footholds (i.e., intelligent test). Assist the HCC Department with:
   i. Validate existing controls and processes implemented to identify a targeted attack;
   ii. Obtain an understanding of its ability to detect and effectively respond to an attack;
   iii. Obtain an understanding of the HCC Department's ability to hinder an attacker from obtaining confidential or sensitive data (e.g., ePHI, PII, financial, privilege, and employee); and,
   iv. Understand the effectiveness of attack scenarios modeled after real world threat intelligence.

b. **External (Internet) Network Penetration Testing**. This will include attempts to obtain confidential customer, sensitive employee data, and other sensitive data from external sources using penetration techniques based on real world threat intelligence. Testing includes, but is not limited to, web applications, firewalls, remote access (e.g., Virtual Private Network and Remote Data Protocol), Internet accessible servers, and Internet postings. Plante Moran will attempt to avoid detection during this phase of testing. Additionally, the Consultant will take actions to evade the HCC Department's efforts to respond to any detection that may occur. Specifically, this will include:
   i. Penetration Testing (i.e. blind and intelligent)
   ii. Vulnerability Assessment
   iii. Potential risks to those identified information assets (to include potential costs of privacy or security breaches and other information security threats), and associated with how the HCC Department collects, uses, manages, stores, maintains, discloses, and disposes of information.
   iv. Physical assessment of technical infrastructure
   v. Identification of potential risks to those identified information assets (to include potential costs of privacy or security breaches and other information security threats), and associated with how the HCC Department collects, uses, manages, stores, maintains, discloses, and disposes of information
   vi. Review existing security measures and report on the effectiveness of those measures
   vii. Identification of potential gaps or deficiencies in maintenance, protection, and utilization of the information assets

viii. Internal/external networks (including penetration tests)
ix. Internet/intranet vulnerability test
x. Internet, Extranet and Intranet applications
xi. Servers and data storage.
xii. Workstations and peripheral endpoints
xiii. Virtual Private Network and remote access infrastructure

c. **Internal Network Penetration Testing**. This will include attempts to obtain confidential customer (ePHI), sensitive employee data, and other sensitive data from internal network sources using penetration techniques based on real world threat intelligence. Testing includes, but is not limited to, servers, workstations, Intranet sites, peripheral endpoints, network devices, storage devices, encryption, and password strength (e.g., password cracking). Consultant will attempt to avoid detection during this phase of testing. Additionally, Consultant must take actions to evade the Department's efforts to respond to any detection that may occur.

Internal testing will be performed utilizing the following pre-determined network foothold assumptions:

- Access from a physical network port without network credentials; and
- Access from an authenticated workstation, simulating a Trojan or successful phishing attack.

Consultant shall perform internal penetration testing and vulnerability scans of the HCC Department's internal network to include those items listed under 1.b. above.

d. **Physical Assessment.** This will review the physical security controls for the information assets that create, receive, maintain or transmit electronic ePHI to validate the HCC Department's current procedures to safeguard sensitive and secured areas and the equipment therein from unauthorized physical access, tampering, theft, and physical elements. Consultant shall perform:
i. Physical assessment of technical infrastructure;
ii. A systematic and thorough identification and evaluation of the County's information assets (data, information systems, and information processing facilities) which create, receive, maintain, or transmit ePHI.

e. **Wireless Penetration Testing**. This will include attempts to obtain confidential member, sensitive employee, and other sensitive data from network sources accessible via the wireless network(s). Consultant must attempt to gain access to the HCC Department's password protected wireless network(s). Consultant shall also test the segmentation of the guest (Internet only) wireless network(s). Consultant must attempt to avoid detection during this phase of testing. Additionally, Consultant must take actions to evade the HCC Department's efforts to respond to any detection that may occur. Specifically, Consultant will test wireless networks, including, but not limited to, secure and guest Wi-Fi access points.

f. **Firewall Review.** Firewall review must analyze firewall configurations and access rules of key firewalls for security vulnerabilities and weaknesses. Specifically, Consultant shall review firewall diagnostics.

g. **Mobile Device.** Consultant will review and analyze security controls implemented for mobile devices that access ePHI.

h. **Denial of Service Test**. Consultant must perform denial of service attacks against HCC Department systems that host sensitive data.

i. **Social Testing**. This will include attempts to obtain confidential customer, sensitive employee data, and other sensitive data from employees using social attack techniques based on real world threat intelligence. Types of social attacks will include spear phishing, phone call impersonation, physical impersonation, piggy-backing, dumpster diving, etc. Consultant must attempt to avoid spam filters, antivirus and other detection mechanisms during this phase of testing.

j. **Security Architecture and Configuration Review.** Consultant must review and analyze security controls implemented in the IT environment by the HCC Department.

k. **Automated Testing**. Through this phase, Consultant must test the effectiveness of the County's vulnerability and patch management programs against known vulnerabilities. The overall objectives are to help each HCC Department:
   i. Identify known vulnerabilities, currently present within their environment;
   ii. Obtain an understanding of the implications of the vulnerabilities identified;
   iii. Where possible, without causing disruption, validate scan results; and
   iv. Provide a filtered end product, which helps management prioritize their remediation efforts.

   Consultant shall focus on the following:
   i. Vulnerability scanning;
   ii. Validation and Prioritization results.

l. **Vulnerability scanning.** Consultant shall help HCC Departments identify known and detectible vulnerabilities present in the external and internal network infrastructure. Vulnerability scanning shall be performed on servers, workstations, web based applications, and other general devices to provide management with an understanding of the HCC Department's exposure to preventable security flaws.

   Consultant shall utilize various automated tools, such as vulnerability scanners to perform the network security review. The tools must be configured not to cause system disruptions or degradation of service. Consultant shall work with the County's/HCC Department's IT department to discuss the specific tools that will be used and the timing for running the tests to minimize any potential impact.

   Consultant shall document all automated and manual tools utilized including the identification if they are commercial, proprietary, or open-source throughout these assessments.

m. **Validation and Prioritization of Results.** This will include an assessment of the vulnerability scanning results. Consultant shall assist the HCC Department with validating, eliminating false positives, filtering and prioritizing the scan output to provide management with relevant scan results detailing known vulnerabilities, which Consultant believes pose a significant risk to the selected systems for focused remediation.

   The output of the review shall be filtered to include critical, high, and moderate issues. Raw scan output shall also be provided in the event management would like to review all issues identified by Consultant's vulnerability scanning tools during the assessment. Scan results shall be provided in native, unfiltered reports and prioritized and curated issues to be included as part of Consultant's Assessment report.

n. **Knowledge Sharing**. Consultant shall provide the HCC Department's technical team with a detailed, step-by-step dissection of Consultant's attack methodology, key learning points, and live demonstrations of select activities and exploitation performed during project execution.

Consultant shall schedule weekly meetings and/or conference calls with the HCC Department to:

i. Report on the status of the project work plan and timeline;
ii. Re-schedule tasks as necessary;
iii. Discuss major open issues/risks and develop strategies to address them; and,
iv. Review next steps.

2. HIPAA Security Rule Gap Analysis (Mandatory) – Consultant shall review the County's current non-technical processes and systems in order to identify potential threats and vulnerabilities that could compromise the confidentiality, integrity and availability of the County information assets. Consultant's evaluation shall include the following technical areas:

a. HIPAA Inventory. Consultant shall develop an understanding of the County HCC Department applications and IT systems that process, store, transmit, and archive PHI data. In addition, Consultant shall develop an understanding of business relationships, contractual arrangements, and agreements in place that may handle or process PHI data on behalf of the County HCC Departments. This will include discussions with key personnel and a review of documentation around business processes that involve PHI data.

b. HIPAA Security Rule Evaluation. Consultant shall evaluate the design of existing controls and identify control gaps based on regulatory compliance requirements. Consultant must ensure evaluation of all required and addressable implementation specifications. During the process, Consultant's evaluation must include the following activities:

i. *§164.306 General Requirements*: Summary of Activities: The scope of the IT Security Policies and Practices assessment must include a review of the HCC Department's current IT administrative policies, processes and procedures in order to gain an understanding of the current IT administrative state as well as identify opportunities to implement IT security best practices.

Consultant shall review existing IT security policy documentation to gain a comprehensive understanding of the current policy administration state, as well as the overall security and administration of IT security policies. The review includes:

- Existing administrative policies and practices;
- Governance structures, initiatives, plans; and
- Projects including those involving internal resources and customers, affiliated entities or agencies and external stakeholders.

Additionally, Consultant shall identify gaps relative to documentation provided. These gaps could apply to a specific IT unit or the County's IT function as a whole.

ii. *164.308 Administrative Safeguards*: Consultant shall evaluate the policies regarding health information, security, compliance with grievances for the County in regards to PHI and HIPAA. This will consist of an evaluation of the HCC Department's policies to ensure compliance with the Department of Health and Human Services, Centers for Medicare and Medicaid Services and program

specific regulations regarding protection of client information. Items analyzed as part of the assessment must include:

1. Review of job descriptions for security and compliance officials;
2. Review of security incidents, police reports and insurance claims;
3. Review of organizational chart;
4. Review of contracted services contracts and requirements;
5. Review of employee orientations, employee in-services and training regarding HIPAA, HITECH and PHI; and
6. Interview of administrator, security and compliance officials.

iii. *164.310 Physical Safeguards*. Consultant shall evaluate the physical measures in place for the HCC Departments in regards to PHI and HIPAA, including evaluation of the County's/HCC Departments' buildings and equipment, and review of policies to protect physical information and media from natural and environmental hazards, and unauthorized intrusion. Items analyzed as part of the assessment must include:

1. Inspection of patient/client intake and registration areas, document processing, and elimination areas;
2. Inspection of HCC Department administrative offices, clinic locations, sub-units and drop sites, and staff vehicle check;
3. Inspection of equipment and property tags and controls;
4. Review of policies to protect information and data; and
5. Interview of staff, clinicians and business associates.

iv. *§164.312 Technical Safeguards*. Consultant shall review existing processes, practices, and controls for security administration. Consultant shall review security practices over the provision of user accounts, management of security hardware and software implemented to monitor and log security activity, and practices over the management of the County data with third party sources. Consultants assessment procedures must include the following:

1. Review security access provisioning procedures, the design of security roles created to support employee's job duties and functions;
2. Verify access rights are updated based upon modifications to job-related responsibilities and the employee;
3. Review security procedures established to manage mobile and remote user access;
4. Determine if sensitive data classifications have been established to identify and define the level of data protection (e.g. PHI segregated and isolated for public access);
5. Review requirements regarding the protection of the County data by third party vendors and contractors;
6. Review security policies and administrative practices implemented to protect the County data and IT systems.

3. Privacy Rule Gap Analysis (Optional) – At the request of an HCC Department, Consultant will analyze information handling practices, specifically information disclosures against the requirements of the HIPAA Privacy Rule and identify gaps between current practices and required practices under HIPAA.

Consultant shall work with each HCC Department to identify its own goals and expected outcomes, or "deliverables." Consultant shall perform the following tasks:

a. PHI Inventory. Consultant shall develop an understanding of HCC Department practices, generation, retention, and destruction of PHI data. In addition, Consultant shall develop an understanding of HCC Department policies and procedures over the administration and management of PHI data. Consultant shall inventory and understand the use of forms and records related to the disclosure of health information.

b. HIPAA Privacy Evaluation.
   i. HIPAA Privacy Compliance Assessment: Consultant shall evaluate the design of existing controls and identify control gaps based on HIPAA Privacy compliance requirements. During this process, the evaluation must include the following activities:
      a) Identify and review procedures and supporting forms, disclosures, and documentation regarding the following HIPAA practice areas:
         1. Use and disclosure of PHI
         2. Minimum necessary requirements
         3. Business Associates and contract agreements
         4. Personal representative arrangements
         5. Use and disclosure of information
         6. Authorization for marketing
         7. De identification/re-identification of PHI
         8. Limited data sets
         9. Data use agreements
         10. Fundraising
         11. Verification of identity and authority
         12. Notice of Information practices
         13. Request for restrictions
         14. Confidential communications requirement
         15. Access to PHI
         16. Amendment of PHI
         17. Accounting of disclosure
         18. Personnel designation
         19. Training Safeguards
         20. Complaints and Grievances
         21. Breach Reporting
         22. Sanctions

4. HIPAA Physical Assessment and End User Security Awareness Assessment (Optional)

a. At the request of an HCC Department, Consultant shall evaluate the physical measures implemented by the HCC Department to control physical access to systems, applications, and health records (electronic and physical). Consultant shall evaluate the HCC Department's buildings and equipment, and review the HCC Department's policies to protect information and media from natural and environmental hazards, and unauthorized intrusion. The assessment shall include:
   i. HIPAA Physical Evaluation. Consultant shall identify and review policies, procedures and supporting forms, disclosures, and documentation regarding the following HIPAA privacy and security areas:
      1. Authorized and limited physical access to locations;
      2. Security methods used to secure sensitive storage locations containing PHI;
      3. Contingencies over physical access during emergency conditions;
      4. Controls used to identify personnel or restricted areas (e.g. visitor badges, signage);

5. Verification of identity and authority;
6. Notice of information practices;
7. Request for restrictions; and
8. Confidential communication requirements.

ii. HIPAA Security Awareness Training Evaluation. Consultant shall identify and review policies, procedures, electronic and manual training aides and current curriculum, and documentation supporting HIPAA Security Awareness Training. Consultants evaluation shall include the following procedures:

1. Review of HCC Department security training materials, program and curriculum;
2. Review of security reminders, notification, and communications;
3. Review of sanctions, policies and practices;
4. Review of security training records management;
5. Review of security training policies and standards; and
6. Notice of information practices.

B. WORKING RELATIONSHIP

1. After execution of the Agreement and prior to commencement of services, Consultant shall participate in a kick-off meeting with representatives from the County and the HCC Departments. The meeting must occur in person at a County facility to be determined, with the Consultant's Project Manager and key members of the project team. The purpose of the meeting is to introduce the Consultant to the HCC Department representatives and establish contacts with the HCC Departments. Consultant shall provide a brief description of Consultant's business and an overview of the services to be provided pursuant to this Agreement.

2. County will provide a Project Steering Committee to advise Consultant's Project Manager (as defined in Section C.3 below) during the project. The Project Steering Committee members will have appropriate management levels representing key interests within each HCC Department.

2. Consultant's personnel shall consist of those individuals whose qualifications were submitted as part of the response to RFP # CAO119-CAO04-3198 HIPAA/HITECH Security Risk Analysis Services, page 21, a copy of which is attached hereto as Exhibit C. Any substitutions of Consultant personnel must be submitted in advance for review by County's Project Manager, who's written Acceptance is required prior to the substitution. County shall have the right to request substitution of Consultant's personnel, including Consultant's Project Manager, upon reasonable request and notice to Consultant. Consultant shall adhere to County's request.

3. Consultant shall identify a full-time dedicated "Consultant's Project Manager," whose role will be to directly oversee performance of the services that are the subject of this Agreement and act as a liaison with County's Project Manager. Consultant's Project Manager shall**:**
   a. Be responsible for conducting a project orientation or "kick-off" meeting in which the schedule, staffing and other elements of the project are presented to and finalized with the Project Steering Committee. A schedule must be finalized at the beginning of the project and updated for submission and comment with each status report.
   b. Establish procedures for interaction between County HCC Department personnel and Consultant, subject to written acceptance by County's Project Manager. Tasks C.4 through C.8 shall be included in the procedures to measure the project's progress, control, quality, and Deliverables.
   c. Be responsive to and work cooperatively with County's Project Manager with respect to the performance of the project.

d. Consultant shall ensure that all information obtained or generated in the course of providing services pursuant to this SOW are kept confidential by all employees and agents of Consultant, and further, that such information, whether or not in reports, documents, presentations or otherwise, is disclosed only to authorized recipients of that information, whether or not the recipient is an agent or employee of County. Consultant shall abide by, and cause each of its employees and agents to abide by, any and all instructions from County as to the limits on distribution of information generated in the course of providing services pursuant to this Agreement.

4. Optional Privacy Rule Gap Analysis (Category 3) and HIPAA Physical Assessment and End User Security Awareness Assessment (Category 4)
   At the request of an HCC Department, Consultant must provide an estimate prior to commencing any work for any HCC Department on Categories 3 and 4 after the initial assessment is done. This estimate shall give consideration as if multiple departments may have a similar request for any of these optional assessment categories within the contract term.

5. Project Steering Committee Meetings
   Formal meetings between Consultant's Project Manager and the Project Steering Committee shall occur on an as needed basis. Consultant shall prepare and distribute written agendas and any supporting materials at least 24 hours prior to the meeting, and meeting minutes within ten days following each meeting. The purposes for the meetings include, but are not limited to, reporting the project status, policy/processing issues, and providing an overview of actions and assessments to be taken during the following period.

6. Status Meetings
   Formal meetings between Consultant personnel (including Consultant's Project Manager) and HCC Department project personnel shall occur as each Milestone is achieved and at 50% completion of each Milestone, unless more frequent meetings are approved by the County's Project Manager.

7. Executive and Staff Briefing
   Consultant shall conduct Executive and staff briefings at the conclusion of each Milestone and at the conclusion of the project. Consultant's Project Manager shall provide an overview of the project status, and provide observations and recommendations concerning future actions with respect to HIPAA compliance. Recommendations that involve reference to risk levels shall include a categorization of each risk in accordance with Exhibit B, along with an explanation for the risk level categorization chosen.

8. Status Reports and Project Plan Requirements
   Consultant's Project Manager shall submit written status reports to County's Project Manager and the respective HCC Department's Project Manager; and shall meet with County's Project Manager and the respective Department's Project Manager during the following designated periods in order to provide reports on the current assessments and Milestones.

   a. First status report. Due to County's Project Manager and each HCC Department's Project Manager seven (7) calendar days after Consultant begins work.

   b. Ongoing Status Reports. Upon completion of each Milestone a status report must be provided to the County's Project Manager and the HCC Department's Project Manager. Within 7 calendar days of submission of the report, a meeting must occur between the Consultant's Project Manager, County's Project Manager and the HCC Department's Project Manager to discuss the status report, plan Tasks, and to address any related matters. The status reports shall include project concerns and alerts related to assessments, audits, or issues.

c. Provide to County's Project Manager and each Department's Project Manager after completion of each Milestone a detailed listing of the assessments, audits, and Deliverables that are scheduled, but have not been completed. Consultant's Project Manager must provide the most current revised due date for completion, and the impact to County if any Task is not completed as scheduled.

d. All reports are to be provided electronically using Microsoft Word.

e. All plans are to be provided electronically using Excel software on CD-ROM and in hard copy. The plans shall include a list of Deliverables, Tasks, and sub-Tasks, each with start and end dates; associated Deliverables for this project, an estimate of fixed costs and Consultant personnel job titles needed to complete each Task. Consultant's Deliverables, Tasks, sub-Tasks and associated Deliverables require written Acceptance of the County's Project Manager and the respective HCC Department's Project Manager.

f. County's Project Manager, or designee, and the HCC Department's Project Manager, as well as the Project Steering Committee, when appropriate, shall have the authority to inspect any and all of Consultant's work in progress. The purpose of such inspections will be to verify project progress as reported by Consultant and to ensure that work products are in conformance with the agreed-upon project requirements. Consultant, at no cost to County, will immediately correct deviations from requirements or contract provisions discovered through such inspections, upon notice from the County.

9. Presentations to each respective Department ascertaining the results of each Milestone.
   A. As described in more detail in Section 6 of this SOW, Consultant shall provide a series of formal Presentations with question and answer segments for each HCC Department, as well as for members from the Information Services Department (ISD), County Counsel, and County Administrative Office (CAO) management and representatives, and other potential invitees.

   B. Presentations are to use Microsoft PowerPoint software as the medium to provide Presentation display screens and handouts. The PowerPoint slides presented must be submitted in electronic format to the County's Project Manager and the appropriate HCC Department's Project Manager. Presentations are subject to prior review and written Acceptance by County's Project Manager and HCC Department's Project Manager. Any Presentation may be provided to other agencies or departments within the County, as deemed appropriate by County's Project Manager.

C. PROJECT MILESTONES, TASKS AND DELIVERABLES

The County Project Team consists of individuals from each HCC Department. The County Project Team also includes individuals from the County Administrative Office (CAO), Information Services Division (ISD), and County Counsel, and others as designated.

The following general requirements are applicable throughout the project. The Consultant Project Team shall:

a. Develop and provide detailed implementation plans for each Deliverable.
b. All Deliverables, including the assessments, impact analysis, gap analysis, status reports, Presentation handouts and all other documentation delivered to County, must be submitted to County's Project Manager for review and with a formal transmittal letter from Consultant's Project Manager.

c. Consultant shall incorporate Milestones 1 thru 4 for each respective HCC Department. Each Milestone Presentation must reference the appropriate appendices for completion of that Milestone:

1. **MILESTONE 1**
   Consultant shall:

   a. **Task 1:** Develop a project work plan that includes a list of Deliverables; Tasks; sub-Tasks with start and end dates and associated Deliverables; an estimate of the number of hours needed to accomplish each Task; and the project job titles of personnel who will complete each of the Tasks identified. The work plan is also to identify Deliverables, Tasks, sub-Tasks, and associated Deliverables which will require written Acceptance by County's Project Manager upon completion.
   Task 1: Deliverables: Project Work Plan - a DETAILED WRITTEN WORK PLAN that covers the entire Project, including each HCC Department.

   b. **Task 2:** Prepare Presentation(s) for the County Project Team regarding Task 1 Deliverables.
   Task 2 Deliverables: Consultant Project Team presents its Project Work Plan and Presentation with handouts to the HCC Departments.

2. **MILESTONE 2**
   Consultant shall:

   a. **Task 3:** Perform Category 1 HIPAA Risk Analysis as described in the SOW for each HCC Department commencing with ISD.
   Task 3 Deliverables: Reports shall include assessment, gap, threat, and vulnerability reports documenting risks and areas requiring improvement, and include recommendations for risk mitigation strategies. The review, analysis, and assessment of administrative vulnerabilities must be described in the reports. Such reports shall be prepared for each HCC Department. For all reports, the findings data shall be made available to County's Project Manager, the applicable HCC Department Project Manager and to the Project Steering Committee upon request. Risk analysis reports must utilize and incorporate Exhibit B Risk Levels.

   b. **Task 4:** Prepare Presentation(s) for the County Project Team regarding Task 3 Deliverables for each HCC Department.

   Task 4 Deliverables: Consultant Project Team presents its Presentations with handouts for Task 3 Deliverables to each HCC Department.

3. **MILESTONE 3**
   Consultant shall:

   a. **Task 5:** Perform Category 2 HIPAA Security Rule Gap Analysis as described in the SOW for each HCC Department commencing with ISD.

   Task 5 Deliverables: Reports shall include assessment, gap, threat, and vulnerability reports documenting the review, analysis, and assessment of technical vulnerabilities that exist. Such reports shall be prepared for each HCC Department. For all reports, the findings data shall be made available to County's Project Manager, the applicable HCC Department Project Manager and to the Project Steering Committee upon request.

b. **Task 6:** Prepare Presentation(s) for the County Project Team regarding Task 5 Deliverables for each HCC Department.

Task 6 Deliverables: Consultant Project Team presents its Presentations with handouts for Task 5 Deliverables to each HCC Department.

4. **MILESTONE 4:**
Consultant shall:

a. **Task 7:** Document the completed project.

b. **Task 7 Deliverables:** Prepare "rough draft" of the Final Project Status Report encompassing all HCC Departments. The Final Project Status Report shall document the entire project, including but not limited to documentation of all assessment results; unresolved problems, unresolved issues, vulnerabilities and recommendations. County's Project Manager, each HCC Department Project Manager, and the Project Steering Committee will review, and may require revisions to, the draft report.

c. **Task 8:** Prepare Presentation(s) for the County Project Team regarding Task 7 Deliverables for each HCC Department; and an overall report that shall include all HCC Departments.

Task 8 Deliverables: Final Project Status Report Presentations and handouts for Task 7 Deliverables shall be prepared for each HCC Department, and a Final Combined Project Status Report Presentation and handouts that include the information from each HCC Department shall be prepared.

d. **Task 9:** Prepare Final Project Status Reports (both Departmental and a combined aggregated executive level summary). Obtain the Acceptance of County's Project Manager (or designee) for all such reports. Obtain each HCC Department Project Manager's Acceptance for each such HCC Department report.

Task 9 Deliverables: Provide the Final Project Status Report. Final compiled report that documents the entire project accomplishments in terms of each HCC Department's report is consolidated into a single report for a County perspective. (Refer to Section 9 of this SOW).

IV. COUNTY RESPONSIBILITIES

A. County shall maintain open and prompt communications with Consultant.

B. County shall designate a project manager that will serve as the primary point of contact for the Consultant.

C. County shall provide the following asset lists to Consultant:
1. Exclusion List - Assets that should never be scanned;
2. Critical Asset List – Assets that Consultant will schedule separately from all other testing activities, schedule a specific time for execution, notify in advance of beginning tests, and then confirm that testing is completed so that all critical services can be confirmed as being in working order.

D. County shall reimburse Consultant in accordance with the Fiscal provisions below.

V. GENERAL AGREEMENT REQUIREMENTS

A. **Recitals**
The recitals set forth above are true and correct and incorporated herein by this reference.

B. **Agreement Amendments**
Consultant agrees any alterations, variations, modifications, or waivers of the provisions of the Agreement, shall be valid only when reduced to writing, executed and attached to the original Agreement and approved by the person(s) authorized to do so on behalf of Consultant and County.

C. **Agreement Assignability**
Without the prior written consent of the County, the Agreement is not assignable by Consultant either in whole or in part.

D. **Agreement Exclusivity**
This is not an exclusive Agreement. The County reserves the right to enter into a contract with other contractors for the same or similar services. The County does not guarantee or represent that the Consultant will be permitted to perform any minimum amount of work, or receive compensation other than on a per order basis, under the terms of this Agreement.

E. **Attorney's Fees and Costs**
If any legal action is instituted to enforce any party's rights hereunder, each party shall bear its own costs and attorney fees, regardless of who is the prevailing party. This paragraph shall not apply to those costs and attorney fees directly arising from a third-party legal action against a party hereto and payable under Indemnification and Insurance Requirements.

F. **Background Checks for Consultant Personnel**
Consultant shall ensure that its personnel (a) are authorized to work in the jurisdiction in which they are assigned to perform Services; (b) do not use legal or illegal substances in any manner which will impact their ability to provide Services to the County; and (c) are not otherwise disqualified from performing the Services under applicable law. If requested by the County and not in violation of applicable law, Consultant shall conduct a background check, at Consultant's sole expense, on all its personnel providing Services. If requested by the County, Consultant shall provide the results of the background check of each individual to the County. Such background check shall be in the form generally used by Consultant in its initial hiring of employees or contracting for Consultants or, as applicable, during the employment-screening process but must, at a minimum, have been performed within the preceding 12-month period. Consultant personnel who do not meet the County's hiring criteria, in County's sole discretion, shall not be assigned to work on County property or Services, and County shall have the right, at its sole option, to refuse access to any Contract personnel to any County facility.

G. **Change of Address**
Consultant shall notify the County in writing, of any change in mailing address within ten (10) business days of the change.

H. **Choice of Law**
This Agreement shall be governed by and construed according to the laws of the State of California.

I. **Compliance with County Policy**
In performing the Services and while at any County facilities, Consultant personnel (including subcontractors) shall (a) conduct themselves in a businesslike manner; (b) comply with the policies, procedures, and rules of the County regarding health and safety, and personal, professional and ethical conduct; (c) comply with the finance, accounting, banking, Internet, security, and/or other applicable standards, policies, practices, processes, procedures, and controls of the County; and (d) abide by all laws applicable to the County facilities and the provision of the Services, and all amendments and modifications to each of the documents listed in subsections (b), (c), and (d)

(collectively, “County Policies”). County Policies, and additions or modifications thereto, may be communicated orally or in writing to Consultant or Consultant personnel or may be made available to Consultant or Consultant personnel by conspicuous posting at a County facility, electronic posting, or other means generally used by County to disseminate such information to its employees or contractors. Consultant shall be responsible for the promulgation and distribution of County Policies to Consultant personnel to the extent necessary and appropriate.

County shall have the right to require Consultant’s employees, agents, representatives and subcontractors to exhibit identification credentials issued by County in order to exercise any right of access under this Agreement.

J. **Confidentiality**

Pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act, regulations have been promulgated governing the privacy of individually identifiable health information. The HIPAA Privacy Rule and Security Rule specify requirements with respect to contracts between a Covered Entity and its Business Associates. Consultant shall execute and comply with the attached Business Associate Agreement (Attachment A). Consultant further agrees to comply with the requirements of other federal and state law that applies to the information collected and maintained by Consultant for Services performed pursuant to Agreement.

K. **Primary Point of Contact**

Consultant will designate an individual to serve as the primary point of contact for the Agreement. Consultant or designee must respond to County inquiries within two (2) business days. Consultant shall not change the primary contact without written acknowledgement to the County. Consultant will also designate a back-up point of contact in the event the primary contact is not available.

L. **County Representative**

The County Chief Operating Officer of his/her designee shall represent the County in all matters pertaining to the services to be rendered under this Agreement, including termination and assignment of this Agreement, and shall be the final authority in all matters pertaining to the Services/Scope of Work by Consultant. If this contract was initially approved by the San Bernardino County Board of Supervisors, then the Board of Supervisors must approve all amendments to this Agreement.

M. **Damage to County Property**

Consultant shall repair, or cause to be repaired, at its own cost, all damages to County vehicles, facilities, buildings or grounds caused by the willful or negligent acts of Consultant or its employees or agents. Such repairs shall be made immediately after Consultant becomes aware of such damage, but in no event later than thirty (30) days after the occurrence.

If the Consultant fails to make timely repairs, the County may make any necessary repairs. The Consultant, as determined by the County, shall repay all costs incurred by the County for such repairs, by cash payment upon demand, or County may deduct such costs from any amounts due to the Consultant from the County, as determined at the County’s sole discretion.

N. **Debarment and Suspension**

Consultant certifies that neither it nor its principals or subcontracts is presently disbarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any federal department or agency. (See the following United States General Services Administration’s System for Award Management website https://www.sam.gov). Consultant further certifies that if it or any of its subcontractors are business entities that must be registered with the California Secretary of State, they are registered and in good standing with the Secretary of State.

O. **Drug and Alcohol Free Workplace**

In recognition of individual rights to work in a safe, healthful and productive work place, as a material condition of this Agreement, the Consultant agrees that the Consultant and the Consultant’s

employees, while performing service for the County, on County property, or while using County equipment:

1. Shall not be in any way impaired because of being under the influence of alcohol or an illegal or controlled substance.

2. Shall not possess an open container of alcohol or consume alcohol or possess or be under the influence of an illegal or controlled substance.

3. Shall not sell, offer, or provide alcohol or an illegal or controlled substance to another person, except where Consultant or Consultant's employee who, as part of the performance of normal job duties and responsibilities, prescribes or administers medically prescribed drugs.

The Consultant shall inform all employees that are performing service for the County on County property, or using County equipment, of the County's objective of a safe, healthful and productive work place and the prohibition of drug or alcohol use or impairment from same while performing such service for the County.

The County may terminate for default or breach of this Agreement and any other Agreement the Consultant has with the County, if the Consultant or Consultant's employees are determined by the County not to be in compliance with above.

P. **Duration of Terms**

This Agreement, and all of its terms and conditions, shall be binding upon and shall inure to the benefit of the heirs, executors, administrators, successors, and assigns of the respective parties, provided no such assignment is in violation of the provisions of this Agreement.

Q. **Employment Discrimination**

During the term of the Agreement, Consultant shall not discriminate against any employee or applicant for employment because of race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, genetic information, marital status, sex, gender, gender identity, gender expression, sexual orientation, age, or military and veteran status. Consultant shall comply with applicable requirements of Executive Orders 11246, 11375, 11625, 12138, 12432, 12250, 13672, Title VI and Title VII of the Civil Rights Act of 1964, the California Fair Employment and Housing Act and other applicable Federal, State and County laws and regulations and policies relating to equal employment and contracting opportunities, including laws and regulations hereafter enacted. Notwithstanding the foregoing, it is agreed that the services to be provided hereunder are not necessary to the performance of any ultimate agreement between the County and federal government and that the Consultant's services here under do not fulfill part of any contract between the federal government and the County. Accordingly, it is likewise also acknowledged and agreed that Consultant is not required to have a written affirmative action plan or to otherwise demonstrate affirmative action compliance as a condition of its performance of the obligations under this Agreement.

R. **Environmental Requirements**

In accordance with County Policy 11-08, the County prefers to acquire and use products with higher levels of post-consumer recycled content. Environmentally preferable goods and materials must perform satisfactorily and be available at a reasonable price. The County requires Consultant to use recycled paper for any printed or photocopied material created as a result of this Agreement. Consultant is also required to use both sides of paper sheets for reports submitted to the County whenever practicable.

To assist the county in meeting the reporting requirements of the California Integrated Waste Management Act of 1989 (AB 939), Consultant must be able to annually report the County's environmentally preferable purchases. Consultant must also be able to report on environmentally preferable goods and materials used in the provision of their service to the County, utilizing a County approved form.

S. **Improper Influence**

Consultant shall make all reasonable efforts to ensure that no County officer or employee, whose position in the County enables him/her to influence any award of the Agreement or any competing offer, shall have any direct or indirect financial interest resulting from the award of the Agreement or shall have any relationship to the Consultant or officer or employee of the Consultant.

T. **Improper Consideration**

Consultant shall not offer (either directly or through an intermediary) any improper consideration such as, but not limited to cash, discounts, service, the provision of travel or entertainment, or any items of value to any officer, employee or agent of the County in an attempt to secure favorable treatment regarding this Agreement.

The County, by written notice, may immediately terminate this Agreement if it determines that any improper consideration as described in the preceding paragraph was offered to any officer, employee or agent of the County with respect to the proposal and award process. This prohibition shall apply to any amendment, extension or evaluation process once a contract has been awarded.

Consultant shall immediately report any attempt by a County officer, employee or agent to solicit (either directly or through an intermediary) improper consideration from Consultant. The report shall be made to the supervisor or manager charged with supervision of the employee or the County Administrative Office. In the event of a termination under this provision, the County is entitled to pursue any available legal remedies.

U. **Informal Dispute Resolution**

In the event the County determines that service is unsatisfactory, or in the event of any other dispute, claim, question or disagreement arising from or relating to this Agreement or breach thereof, the parties hereto shall use their best efforts to settle the dispute, claim, question or disagreement. To this effect, they shall consult and negotiate with each other in good faith and, recognizing their mutual interests, attempt to reach a just and equitable solution satisfactory to both parties.

V. **Legality and Severability**

The parties' actions under the Agreement shall comply with all applicable laws, rules, regulations, court orders and governmental agency orders. The provisions of this Agreement are specifically made severable. If a provision of the Agreement is terminated or held to be invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions shall remain in full effect.

W. **Licenses, Permits and/or Certifications**

Consultant shall maintain all necessary licenses, permits and/or certifications required by the laws of Federal, State, County, and municipal laws, ordinances, rules and regulations. The Consultant shall maintain these licenses, permits and/or certifications in effect for the duration of this Agreement. Consultant will notify County immediately of loss or suspension of any such licenses, permits and/or certifications. Failure to maintain a required license, permit and/or certification may result in immediate termination of this Agreement.

X. **Material Misstatement/Misrepresentation**

If during the course of the administration of this Agreement, the County determines that Consultant has made a material misstatement or misrepresentation or that materially inaccurate information has been provided to the County, this Agreement may be immediately terminated. If this Agreement is terminated according to this provision, the County is entitled to pursue any available legal remedies.

Y. **Mutual Covenants**

The parties to this Agreement mutually covenant to perform all of their obligations hereunder, to exercise all discretion and rights granted hereunder, and to give all consents in a reasonable manner consistent with the standards of "good faith" and "fair dealing".

Z. **Nondisclosure**

Consultant shall hold as confidential and use reasonable care to prevent unauthorized access by, storage, disclosure, publication, dissemination to and/or use by third parties of, confidential information that is either: (1) provided by the County to Consultant or an agent of Consultant or otherwise made available to Consultant or Consultant's agent in connection with this Agreement; or, (2) acquired, obtained, or learned by Consultant or an agent of Consultant in the performance of this Agreement. For purposes of this provision, confidential information means any data, files, software, information or materials in oral, electronic, tangible or intangible form and however stored, compiled or memorialize and includes, but is not limited to, technology infrastructure, architecture, financial data, trade secrets, equipment specifications, user lists, passwords, research data, and technology data.

AA. **Notice of Delays**

Except as otherwise provided herein, when either party has knowledge that any actual or potential situation is delaying or threatens to delay the timely performance of this contract, that party shall, within twenty-four (24) hours, give notice thereof, including all relevant information with respect thereto, to the other party.

BB. **Ownership of Documents**

To the extent created and intended for delivery to the County, all documents, data, products, graphics, computer programs and reports prepared by Consultant pursuant to the Agreement shall be considered property of the County upon payment for services (and products, if applicable). All such items shall be delivered to County at the completion of work under the Agreement, subject to the requirements of Section VI – Term of Agreement. Unless otherwise directed by County, Consultant may retain copies of such items.

CC. **Air, Water Pollution Control, Safety and Health**

Consultant shall comply with all air pollution control, water pollution, safety and health ordinances and statutes, which apply to the work performed pursuant to this Agreement.

DD. **Records**

Consultant shall maintain all records and books pertaining to the delivery of services under this Agreement and demonstrate accountability for contract performance. All records shall be complete and current and comply with all Agreement requirements. Failure to maintain acceptable records shall be considered grounds for withholding of payments for invoices submitted and/or termination of the Agreement.

All records relating to the Consultant's personnel, consultants, subcontractors, Services/Scope of Work and expenses pertaining to this Agreement shall be kept in a generally acceptable accounting format. Records should include primary source documents. Fiscal records shall be kept in accordance with Generally Accepted Accounting Principles and must account for all funds, tangible assets, revenue and expenditures. Fiscal records must comply with the appropriate Office of Management and Budget (OMB) Circulars, which state the administrative requirements, cost principles and other standards for accountancy.

EE. **Relationship of the Parties**

Nothing contained in this Agreement shall be construed as creating a joint venture, partnership, or employment arrangement between the Parties hereto, nor shall either Party have the right, power or authority to create an obligation or duty, expressed or implied, on behalf of the other Party hereto.

FF. **Release of Information**

No news releases, advertisements, public announcements or photographs arising out of the Agreement or Consultant's relationship with County may be made or used without prior written approval of the County.

GG. **Representation of the County**

In the performance of this Agreement, Consultant, its agents and employees, shall act in an independent capacity and not as officers, employees, or agents of the County of San Bernardino.

HH. **Strict Performance**
Failure by a party to insist upon the strict performance of any of the provisions of this Agreement by the other party, or the failure by a party to exercise its rights upon the default of the other party, shall not constitute a waiver of such party's right to insist and demand strict compliance by the other party with the terms of this Agreement thereafter.

II. **Subcontracting**
Consultant shall not utilize a subcontractor for services performed pursuant to this Agreement.

JJ. **Subpoena**
In the event that a subpoena or other legal process commenced by a third party in any way concerning the Goods or Services provided under this Agreement is served upon Consultant or County, such party agrees to notify the other party in the most expeditious fashion possible following receipt of such subpoena or other legal process. Consultant and County further agree to cooperate with the other party in any lawful effort by such other party to contest the legal validity of such subpoena or other legal process commenced by a third party as may be reasonably required and at the expense of the party to whom the legal process is directed, except as otherwise provided herein in connection with defense obligations by Consultant for County.

KK. **Time of the Essence**
Time is of the essence in performance of this Agreement and of each of its provisions.

LL. **Venue**
The parties acknowledge and agree that this Agreement was entered into and intended to be performed in San Bernardino County, California. The parties agree that the venue of any action or claim brought by any party to this Agreement will be the Superior Court of California, County of San Bernardino, San Bernardino District. Each party hereby waives any law or rule of the court, which would allow them to request or demand a change of venue. If any action or claim concerning this Agreement is brought by any third party and filed in another venue, the parties hereto agree to use their best efforts to obtain a change of venue to the Superior Court of California, County of San Bernardino, San Bernardino District.

MM. **Conflict of Interest**
Consultant shall make all reasonable efforts to ensure that no conflict of interest exists between its officers, employees, or subcontractors and the County. Consultant shall make a reasonable effort to prevent employees, Consultant, or members of governing bodies from using their positions for purposes that are, or give the appearance of being motivated by a desire for private gain for themselves or others such as those with whom they have family business, or other ties. Officers, employees, and agents of cities, counties, districts, and other local agencies are subject to applicable conflict of interest codes and state law. In the event the County determines a conflict of interest situation exists, any increase in costs, associated with the conflict of interest situation, may be disallowed by the County and such conflict may constitute grounds for termination of the Agreement. This provision shall not be construed to prohibit employment of persons with whom Consultant's officers, employees, or agents have family, business, or other ties so long as the employment of such persons does not result in increased costs over those associated with the employment of any other equally qualified applicant.

NN. **Former County Administrative Officials**
Consultant agrees to provide, or has already provided information on former County of San Bernardino administrative officials (as defined below) who are employed by or represent Consultant. The information provided includes a list of former County administrative officials who terminated County employment within the last five years and who are now officers, principals, partners, associates or members of the business. The information also includes the employment with or

representation of Consultant. For purposes of this provision, "County administrative official" is defined as a member of the Board of Supervisors or such officer's staff, County Executive Officer or member of such officer's staff, County department or group head, assistant department or group head, or any employee in the Exempt Group, Management Unit or Safety Management Unit.

OO. **Disclosure of Criminal and Civil Procedures**

The County reserves the right to request the information described herein from the Consultant. Failure to provide the information may result in a termination of the Agreement. The County also reserves the right to obtain the requested information by way of a background check performed by an investigative firm. The Consultant also may be requested to provide information to clarify initial responses. Negative information discovered may result in Agreement termination.

Consultant is required to disclose whether the firm, or any of its partners, principals, members, associates or key employees (as that term is defined herein), within the last ten years, has been indicted on or had charges brought against it or them (if still pending) or convicted of any crime or offense arising directly or indirectly from the conduct of the firm's business, or whether the firm, or any of its partners, principals, members, associates or key employees, has within the last ten years, been indicted on or had charges brought against it or them (if still pending) or convicted of any crime or offense involving financial misconduct or fraud. If the response is affirmative, the Consultant will be asked to describe any such indictments or charges (and the status thereof), convictions and the surrounding circumstances in detail.

In addition, the Consultant is required to disclose whether the firm, or any of its partners, principals, members, associates or key employees, within the last ten years, has been the subject of legal proceedings as defined herein arising directly from the provision of services by the firm or those individuals. "Legal proceedings" means any civil actions filed in a court of competent jurisdiction, or any matters filed by an administrative or regulatory body with jurisdiction over the firm or the individuals. If the response is affirmative, the Consultant will be asked to describe any such legal proceedings (and the status and disposition thereof) and the surrounding circumstances in detail.

For purposes of this provision "key employees" includes any individuals providing direct service to the County. "Key employees" do not include clerical personnel providing service at the firm's offices or locations.

PP. **Copyright**

County shall have a royalty-free, non-exclusive and irrevocable license to publish, disclose, copy, translate, and otherwise use, copyright or patent, now and hereafter, all reports, studies, information, data, statistics, forms, designs, plans, procedures, systems, and any other materials or properties developed under this Agreement including those covered by copyright, and reserves the right to authorize others to use or reproduce such material. All such materials developed under the terms of this Agreement shall acknowledge the County of San Bernardino as the funding agency and Consultant as the creator of the publication. No such materials, or properties produced in whole or in part under this Agreement shall be subject to private use, copyright or patent right by Consultant in the United States or in any other country without the express written consent of County. Copies of all educational and training materials, curricula, audio/visual aids, printer material, and periodicals, assembled pursuant to this Agreement must be filed with the County prior to publication.

QQ. **Artwork, Proofs and Negatives**

All artwork, proofs, and/or negatives in either print or digital format for anything produced under the terms of this Agreement are the property of the County. These items must be returned to the County within ten (10) days, upon written notification to the Consultant. In the event of a failure to return the documents, the County is entitled to pursue any available legal remedies. In addition, the Consultant will be barred from all future solicitations, for a period of at least six (6) months.

RR. **Iran Contracting Act**

IRAN CONTRACTING ACT OF 2010, Public Contract Code sections 2200 et seq. (Applicable for all Contracts of one million dollars ($1,000,000) or more). In accordance with Public Contract Code section 2204(a), the Consultant certifies that at the time the Agreement is signed, the Consultant signing the Agreement is not identified on a list created pursuant to subdivision (b) of Public Contract Code section 2203 as a person (as defined in Public Contract Code section 2202(e)) engaging in investment activities in Iran described in subdivision (a) of Public Contract Code section 2202.5, or as a person described in subdivision (b) of Public Contract Code section 2202.5, as applicable.

Consultants are cautioned that making a false certification may subject the Consultant to civil penalties, termination of existing contract, and ineligibility to bid on a contract for a period of three (3) years in accordance with Public Contract Code section 2205.

VI. INDEMNIFICATION AND INSURANCE REQUIREMENTS

A. Indemnification

The Consultant agrees to indemnify, defend (with counsel reasonably approved by County) and hold harmless the County and its authorized officers, employees, agents and volunteers from any and all claims, actions, losses, damages and/or liability arising out of this Agreement to the extent caused by the passive and active negligence or willful misconduct of Consultant and for any costs or expenses incurred by the County on account of any claim except where such indemnification is prohibited by law.

B. Additional Insured

All policies, except for Worker's Compensation, Errors and Omissions and Professional Liability policies shall contain additional endorsements naming the County and its officers, employees, agents and volunteers as additional named insured with respect to liabilities arising out of the performance of services hereunder. The additional insured endorsements shall not limit the scope of coverage for the County to vicarious liability but shall allow coverage for the County to the full extent provided by the policy. Such additional insured coverage shall be at least as broad as Additional Insured (Form B) endorsement form ISO, CG 2010.11 85.

C. Waiver of Subrogation Rights

The Consultant shall require the carriers of required coverages to waive all rights of subrogation against the County, its officers, employees, agents, volunteers, contractors and subcontractors. All general or auto liability insurance coverage provided shall not prohibit the Consultant and Consultant's employees or agents from waiving the right of subrogation prior to a loss or claim. The Consultant hereby waives all rights of subrogation against the County.

D. Policies Primary and Non-Contributory

All policies required herein are to be primary and non-contributory with any insurance or self-insurance programs carried or administered by the County.

E. Severability of Interests

The Consultant agrees to ensure that coverage provided to meet these requirements is applicable separately to each insured and there will be no cross liability exclusions that preclude coverage for suits between the Consultant and the County or between the County and any other insured or additional insured under the policy.

F. Proof of Coverage

The Consultant shall furnish Certificates of Insurance to the County Department administering the Agreement evidencing the insurance coverage at the time the Agreement is executed, additional endorsements, as required shall be provided prior to the commencement of performance of services hereunder, Consultant agrees that such insurance shall not be terminated or expire without thirty (30) days written notice to the Department, and Consultant shall maintain such insurance from the time Consultant commences performance of services hereunder until the completion of such services. Within fifteen (15) days of the commencement of this Agreement, the Consultant shall

furnish a copy of the Declaration page for all applicable policies and will provide complete certified copies of the policies and endorsements immediately upon request.

G. Acceptability of Insurance Carrier
Unless otherwise approved by Risk Management, insurance shall be written by insurers authorized to do business in the State of California and with a minimum "Best" Insurance Guide rating of "A-VII" except that insurance markets based in London, and/or the domestic surplus lines markets that operate on a non-admitted basis are exempt from this requirement, provided that the Consultant's broker can provide financial data to establish that a market is equal to or exceeds the financial strengths associated with the A.M. Best's rating of A-VII or better.

H. Deductibles and Self-Insured Retention
Any and all deductibles or self-insured retentions in excess of $10,000 shall be declared to and approved by Risk Management.

I. Failure to Procure Coverage
In the event that any policy of insurance required under this Agreement does not comply with the requirements, is not procured, or is canceled and not replaced, the County has the right but not the obligation or duty to cancel the Agreement if it deems necessary.

J. Insurance Review
Insurance requirements are subject to periodic review by the County. The Director of Risk Management or designee is authorized, but not required, to reduce, waive or suspend any insurance requirements whenever Risk Management determines that any of the required insurance is not available, is unreasonably priced, or is not needed to protect the interests of the County. In addition, if the Department of Risk Management determines that heretofore unreasonably priced or unavailable types of insurance coverage or coverage limits become reasonably priced or available, the Director of Risk Management or designee is authorized, but not required, to change the above insurance requirements to require additional types of insurance coverage or higher coverage limits, provided that any such change is reasonable in light of past claims against the County, inflation, or any other item reasonably related to the County's risk.

a. Any change requiring additional types of insurance coverage or higher coverage limits must be made by amendment to this Agreement. Consultant agrees to execute any such amendment within thirty (30) days of receipt.

b. Any failure, actual or alleged, on the part of the County to monitor or enforce compliance with any of the insurance and indemnification requirements will not be deemed as a waiver of any rights on the part of the County.

K. The Consultant agrees to provide insurance set forth in accordance with the requirements herein. If the Consultant uses existing coverage to comply with these requirements and that coverage does not meet the specified requirements, the Consultant agrees to amend, supplement or endorse the existing coverage to do so.

Without in anyway affecting the indemnity herein provided and in addition thereto, the Consultant shall secure and maintain throughout the contract term the following types of insurance with limits as shown:

L. Workers' Compensation/Employer's Liability – A program of Workers' Compensation insurance or a state-approved, self-insurance program in an amount and form to meet all applicable requirements of the Labor Code of the State of California, including Employer's Liability with $250,000 limits covering all persons including volunteers providing services on behalf of the Consultant and all risks to such persons under this Agreement.

a. If Consultant has no employees, it may certify or warrant to the County that it does not currently have any employees or individuals who are defined as "employees" under the Labor Code and the requirement for Workers' Compensation coverage will be waived by the County's Director of Risk Management.
b. With respect to Consultants that are non-profit corporations organized under California or Federal law, volunteers for such entities are required to be covered by Workers' Compensation insurance.

M. Commercial/General Liability Insurance – The Consultant shall carry General Liability Insurance covering all operations performed by or on behalf of the Consultant providing coverage for bodily injury and property damage with a combined single limit of not less than one million dollars ($1,000,000), per occurrence. Subject to customary exclusions, exceptions, and limitations, the policy coverage shall include:
a. Premises operations and mobile equipment.
b. Products and completed operations.
c. Broad form property damage (including completed operations).
d. Explosion, collapse and underground hazards.
e. Personal injury.
f. Contractual liability.
g. $2,000,000 general aggregate limit.

N. Automobile Liability Insurance – Primary insurance coverage shall be written on ISO Business Auto coverage form for all owned, hired and non-owned automobiles or symbol 1 (any auto). The policy shall have a combined single limit of not less than one million dollars ($1,000,000) for bodily injury and property damage, per occurrence.

a. If the Consultant is transporting one or more non-employee passengers in performance of contract services, the automobile liability policy shall have a combined single limit of two million dollars ($2,000,000) for bodily injury and property damage per occurrence.
b. If the Consultant owns no autos, a non-owned auto endorsement to the General Liability policy described above is acceptable.

O. Umbrella Liability Insurance – An umbrella (over primary) or excess policy may be used to comply with limits or other primary coverage requirements. When used, the umbrella policy shall apply to bodily injury/property damage, personal injury/advertising injury and shall include a "dropdown" provision providing primary coverage for any liability not covered by the primary policy. The coverage shall also apply to automobile liability.

P. Professional Liability – Professional Liability Insurance with limits of not less than one million ($1,000,000) per claim and two million ($2,000,000) aggregate limits

a. or

Errors and Omissions Liability Insurance – Errors and Omissions Liability Insurance with limits of not less than one million ($1,000,000) and two million ($2,000,000) aggregate limits

b. or

Directors and Officers Insurance coverage with limits of not less than one million ($1,000,000) shall be required for Contracts with charter labor committees or other not-for-profit organizations advising or acting on behalf of the County.

If insurance coverage is provided on a "claims made" policy, the "retroactive date" shall be shown and must be before the date of the state of the contract work. The claims made insurance shall be maintained or "tail" coverage provided for a minimum of five (5) years after contract completion.

Q. Cyber Liability Insurance - Cyber Liability Insurance with limits of no less than $1,000,000 for each occurrence or event with an annual aggregate of $2,000,000 covering privacy violations, information theft, damage to or destruction of electronic information, intentional and/or unintentional release of private information, alteration of electronic information, extortion and network security. The policy shall protect the involved County entities and cover breach response cost as well as regulatory fines and penalties.

VII. FISCAL PROVISIONS

A. The maximum amount of reimbursement under this Agreement shall not exceed $603,000, consisting of the fees detailed on Attachment B, which amount is inclusive of all travel fees, and shall be subject to availability of other funds to the County. The consideration to be paid to Consultant, as provided herein, shall be in full payment for all Consultant's services and expenses incurred in the performance hereof, including travel and per diem.

   a. Categories 3 and 4 line items cost are stated as "not to exceed costs" as illustrated in the Best and Final Offer.

   Invoices shall be submitted monthly in arrears that include an itemization referencing the Project milestone/task/deliverable consistent with the Scope of Work comprised of the department name that services were rendered to, the length of time spent on the identified services, milestones, tasks, and deliverables completed.

B. Consultant shall accept all payments from County via electronic funds transfer (EFT) directly deposited into the Consultant's designated checking or other bank account. Consultant shall promptly comply with directions and accurately complete forms provided by County required to process EFT payments.

C. County is exempt from Federal excise taxes and no payment shall be made for any personal property taxes levied on Consultant or on any taxes levied on employee wages. The County shall only pay for any State or local sales or use taxes on the services rendered or equipment and/or parts supplied to the County pursuant to the Agreement.

D. County shall pay undisputed invoices within 60 days of receipt.

E. Costs for services under the terms of this Agreement shall be incurred during the Agreement period except as approved by County. Consultant shall not use current year funds to pay prior or future year obligations.

F. Consultant shall adhere to the County's Travel Management Policy (8-02 and 08-02SP1) when travel is pursuant to this Agreement and for which reimbursement is sought from the County. In addition, Consultant is encouraged to utilize local transportation services, including but not limited to, the Ontario International Airport.

VIII. RIGHT TO MONITOR AND AUDIT

A. The County, State and Federal government shall have absolute right to review and audit all records, books, papers, documents, corporate minutes, and other pertinent items as requested, and shall have absolute right to monitor the performance of Consultant in the delivery of services provided under this Agreement. Consultant shall give full cooperation, in any auditing or monitoring conducted. Consultant shall cooperate with the County in the implementation, monitoring, and evaluation of this Agreement and comply with any and all reporting requirements established by the County.

B. All records pertaining to services delivered and all fiscal, statistical and management books and records shall be available for examination and audit by County representatives for a period of three

years after final payment under this Agreement or until all pending County, State and Federal audits are completed, whichever is later.

IX. CORRECTION OF PERFORMANCE DEFICIENCIES

A. Failure by Consultant to comply with any of the provisions, covenants, requirements or conditions of this Agreement shall be a material breach of this Agreement.

B. In the event of a non-cured breach, County may, at its sole discretion and in addition to any other remedies available at law, in equity, or otherwise specified in this Agreement:
   1. Afford Consultant thereafter a time period within which to cure the breach, which period shall be established at the sole discretion of County; and/or
   2. Discontinue reimbursement to Consultant for and during the period in which Consultant is in breach, which reimbursement shall not be entitled to later recovery; and/or
   3. Withhold funds pending duration of the breach; and/or
   4. Offset against any monies billed by Consultant but yet unpaid by County those monies disallowed pursuant to Item “b” of this paragraph; and/or
   5. Terminate this Agreement immediately and be relieved of the payment of any consideration to Consultant. In the event of such termination, the County may proceed with the work in any manner deemed proper by the County. The cost to the County shall be deducted from any sum due to the Consultant under this Agreement and the balance, if any, shall be paid by the Consultant upon demand.

X. TERM OF AGREEMENT

This Agreement is effective as of February 11, 2020 and expires February 10, 2021, with three, one-year options to extend, but may be terminated earlier in accordance with provisions of this Agreement. All options to extend require an amendment to the Agreement approved by the Board of Supervisors and Consultant.

The County and the Consultant each reserve the right to terminate the Agreement, for any reason, with a thirty (30) day written notice of termination. Such termination may include all or part of the services described herein. Upon such termination, payment will be made to the Consultant for services rendered and expenses reasonably incurred prior to the effective date of termination. Upon receipt of termination notice Consultant shall promptly discontinue services unless the notice directs otherwise. Consultant shall deliver promptly to County and transfer title (if necessary) all completed work, and work in progress, including drafts, documents, plans, forms, data, products, graphics, computer programs and reports.

XI. EARLY TERMINATION

A. The County may terminate the Agreement immediately under the provisions of Section X – Paragraph B, Item 5 of the Agreement. In addition, the Agreement may be terminated without cause by the County by serving a written notice to the Consultant thirty (30) days in advance of termination. The Chief Operating Officer is authorized to exercise the County’s right with respect to any termination of this Agreement.

B. Consultant shall only be reimbursed for costs and uncancelable obligations incurred prior to the date of termination. Consultant shall not be reimbursed for costs incurred after the date of termination.

C. Upon receipt of termination notice, Consultant shall promptly discontinue services unless the notice directs otherwise. Consultant shall deliver promptly to County and transfer title (if necessary) all completed work, and work in progress, including drafts, documents, plans, forms, data, products, graphics, computer programs, and reports.

XII. NOTICES

All written notices provided for in this Agreement or which either party desires to give to the other shall be deemed fully given, when made in writing and either served personally, or by facsimile, or deposited in the United States mail, postage prepaid, and addressed to the other party as follows:

County of San Bernardino
County Administrative Office
385 N. Arrowhead Avenue, 5th Floor
San Bernardino, CA 92415-0120

Plante & Moran, PLLC
3000 Town Center Suite 400
Southfield, MI 48034

Notice shall be deemed communicated two (2) County working days from the time of mailing if mailed as provided in this paragraph.

XIII. ENTIRE AGREEMENT

This Agreement, including all Exhibits and other attachments, which are attached hereto and incorporated by reference, and other documents incorporated herein, represents the final, complete and exclusive agreement between the parties hereto. Any prior agreement, promises, negotiations or representations relating to the subject matter of this Agreement not expressly set forth herein are of no force or effect. This Agreement is executed without reliance upon any promise, warranty or representation by any party or any representative of any party other than those expressly contained herein. Each party has carefully read this Agreement and signs the same of its own free will.

IN WITNESS WHEREOF, the County of San Bernardino and the Consultant have each caused this Agreement to be subscribed by its respective duly authorized officers, on its behalf.

COUNTY OF SAN BERNARDINO

►

Curt Hagman, Chairman, Board of Supervisors

Dated:

SIGNED AND CERTIFIED THAT A COPY OF THIS DOCUMENT HAS BEEN DELIVERED TO THE CHAIRMAN OF THE BOARD

Lynna Monell
Clerk of the Board of Supervisors
of the County of San Bernardino

By

Deputy

Plante & Moran, PLLC
(Print or type name of corporation, company, contractor, etc.)

By ►

(Authorized signature - sign in blue ink)

Name Raj Patel
(*Print or type name of person signing contract)*

Title Management Consulting Partner
(Print or Type)

Dated:

Address 3000 Town Center Suite 400,
Southfield, MI 48034

FOR COUNTY USE ONLY

Approved as to Legal Form	Reviewed for Contract Compliance	Reviewed/Approved by Department
►	►	►
County Counsel		
Date	Date	Date

ATTACHMENT A
BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (Agreement) supplements and is made a part of the contract (Contract) by and between the County of San Bernardino (hereinafter Covered Entity) and Plante & Moran, PLLC (hereinafter Business Associate). This Agreement is effective as of the effective date of the Contract.

RECITALS

WHEREAS, Covered Entity (CE) wishes to disclose certain information to Business Associate (BA) pursuant to the terms of the Contract, which may include Protected Health Information (PHI); and

WHEREAS, CE and BA intend to protect the privacy and provide for the security of the PHI disclosed to BA 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 (HITECH Act), their implementing regulations, and other applicable laws; and

WHEREAS, The Privacy Rule and the Security Rule require CE to enter into a contract containing specific requirements with BA prior to the disclosure of PHI, as set forth in, but not limited to, Title 45, sections 164.314, subdivision (a), 164.502, subdivision (e), and 164.504, subdivision (e) of the Code of Federal Regulations (C.F.R.) and contained in this Agreement; and

WHEREAS, Pursuant to HIPAA and the HITECH Act, BA shall fulfill the responsibilities of this Agreement by being in compliance with the applicable provisions of the HIPAA Standards for Privacy of PHI set forth at 45 C.F.R. sections 164.308 (Administrative Safeguards), 164.310 (Physical Safeguards), 164.312 (Technical Safeguards), 164.316 (Policies and Procedures and Documentation Requirements), and, 164.400, et seq. and 42 United States Code (U.S.C.) section 17932 (Breach Notification Rule), in the same manner as they apply to a CE under HIPAA;

NOW THEREFORE, in consideration of the mutual promises below and the exchange of information pursuant to this Agreement, the parties agree as follows:

A. Definitions

Unless otherwise specified herein, capitalized terms used in this Agreement shall have the same meanings as given in the Privacy Rule, the Security Rule, the Breach Notification Rule, and HITECH Act, as and when amended from time to time.

1. Breach shall have the same meaning given to such term under the HIPAA Regulations [45 C.F.R. §164.402] and the HITECH Act [42 U.S.C. §§17921 et seq.], and as further described in California Civil Code section 1798.82.
2. Business Associate (BA) shall have the same meaning given to such term under the Privacy Rule, the Security Rule, and the HITECH Act, including but not limited to 42 U.S.C. section 17921 and 45 C.F.R. section 160.103.
3. Covered Entity (CE) shall have the same meaning given to such term as under the Privacy Rule and Security Rule, including, but not limited to 45 C.F.R. section 160.103.
4. Designated Record Set shall have the same meaning given to such term under 45 C.F.R. section 164.501.
5. Electronic Protected Health Information (ePHI) means PHI that is maintained in or transmitted by electronic media as defined in the Security Rule, 45 C.F.R. section 164.103.
6. Individual shall have the same meaning given to such term under 45 C.F.R. section 160.103.
7. Privacy Rule means the regulations promulgated under HIPAA by the United States Department of Health and Human Services (HHS) to protect the privacy of Protected Health Information, including, but not limited to, 45 C.F.R. Parts 160 and 164, subparts A and E.

8. Protected Health Information (PHI) shall have the same meaning given to such term under 45 C.F.R. section 160.103, limited to the information received from, or created or received by Business Associate from or on behalf of, CE.

9. Security Rule means the regulations promulgated under HIPAA by HHS to protect the security of ePHI, including, but not limited to, 45 C.F.R. Part 160 and 45 C.F.R. Part 164, subparts A and C.

10. Unsecured PHI shall have the same 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, subdivision (h).

B. Obligations and Activities of BA

1. Permitted Uses and Disclosures

BA may disclose PHI: (i) for the proper management and administration of BA; (ii) to carry out the legal responsibilities of BA; (iii) for purposes of Treatment, Payment and Operations (TPO); (iv) as required by law; or (v) for Data Aggregation purposes for the Health Care Operations of CE. Prior to making any other disclosures, BA must obtain a written authorization from the Individual.

If BA discloses PHI to a third party, BA must obtain, prior to making any such disclosure, (i) reasonable written assurances from such third party that such PHI will be held confidential as provided pursuant to this Agreement and only disclosed as required by law or for the purposes for which it was disclosed to such third party, and (ii) a written agreement from such third party to immediately notify BA of any breaches of confidentiality of the PHI, 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)]

2. Prohibited Uses and Disclosures

i. BA shall not use, access or further disclose PHI other than as permitted or required by this Agreement and as specified in the attached Contract or as required by law. Further, BA shall not use PHI in any manner that would constitute a violation of the Privacy Rule or the HITECH Act. BA shall disclose to its employees, subcontractors, agents, or other third parties, and request from CE, only the minimum PHI necessary to perform or fulfill a specific function required or permitted hereunder.

ii. BA shall not use or disclose PHI for fundraising or marketing purposes.

iii. BA shall not disclose PHI 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) and 45 C.F.R. section 164.522(a)(1)(i)(A).)

iv. BA shall not directly or indirectly receive remuneration in exchange for PHI, except with the prior written consent of CE and as permitted by the HITECH Act (42 U.S.C. section 17935(d)(2); and 45 C.F.R. section 164.508); however, this prohibition shall not affect payment by CE to BA for services provided pursuant to this Agreement.

3. Appropriate Safeguards

i. BA shall implement appropriate safeguards to prevent the unauthorized use or disclosure of PHI, including, but not limited to, administrative, physical and technical safeguards that reasonably protect the confidentiality, integrity and availability of the PHI BA creates, receives, maintains, or transmits on behalf of the CE, in accordance with 45 C.F.R. sections 164.308, 164.310, 164.312 and 164.316. [45 C.F.R. sections 164.504(e)(2)(ii)(b) and 164.308(b).]

ii. In accordance with 45 C.F.R. section 164.316, BA shall maintain reasonable and appropriate written policies and procedures for its privacy and security program in order to comply with the standards, implementation specifications, or any other requirements of the Privacy Rule and applicable provisions of the Security Rule.

iii. BA shall provide appropriate training for its workforce on the requirements of the Privacy Rule and Security Rule as those regulations affect the proper handling, use confidentiality and disclosure of the CE's PHI.

Such training will include specific guidance relating to sanctions against workforce members who fail to comply with privacy and security policies and procedures and the obligations of the BA under this Agreement.

4. Subcontractors

BA shall enter into written agreements with agents and subcontractors to whom BA provides CE's PHI that impose the same restrictions and conditions on such agents and subcontractors that apply to BA with respect to such PHI, and that require compliance with all appropriate safeguards as found in this Agreement.

5. Reporting of Improper Access, Use or Disclosure or Breach

Every suspected and actual Breach shall be reported immediately, but no later than one (1) business day upon discovery, to CE's Office of Compliance, consistent with the regulations under HITECH Act. Upon discovery of a Breach or suspected Breach, BA shall complete the following actions:

i. Provide CE's Office of Compliance with the following information to include but not limited to:

a) Date the Breach or suspected Breach occurred;

b) Date the Breach or suspected Breach was discovered;

c) Number of staff, employees, subcontractors, agents or other third parties and the names and titles of each person allegedly involved;

d) Number of potentially affected Individual(s) with contact information; and

e) Description of how the Breach or suspected Breach allegedly occurred.

ii. Conduct and document a risk assessment by investigating without unreasonable delay and in no case later than five (5) calendar days of discovery of the Breach or suspected Breach to determine the following:

a) The nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification;

b) The unauthorized person who had access to the PHI;

c) Whether the PHI was actually acquired or viewed; and

d) The extent to which the risk to PHI has been mitigated.

iii. Provide a completed risk assessment and investigation documentation to CE's Office of Compliance within ten (10) calendar days of discovery of the Breach or suspected Breach with a determination as to whether a Breach has occurred. At the discretion of CE, additional information may be requested.

a) If BA and CE agree that a Breach has not occurred, notification to Individual(s) is not required.

b) If a Breach has occurred, notification to the Individual(s) is required and BA must provide CE with affected Individual(s) name and contact information so that CE can provide notification.

iv. Make available to CE and governing State and Federal agencies in a time and manner designated by CE or governing State and Federal agencies, any policies, procedures, internal practices and records relating to a Breach or suspected Breach for the purposes of audit or should the CE reserve the right to conduct its own investigation and analysis.

6. Access to PHI

To the extent BA maintains a Designated Record Set on behalf of CE, BA shall make PHI maintained by BA 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. If BA maintains ePHI, BA shall provide such information in electronic format to enable CE to fulfill

its obligations under the HITECH Act. If BA receives a request from an Individual for access to PHI, BA shall immediately forward such request to CE.

7. Amendment of PHI

   If BA maintains a Designated Record Set on behalf of the CE, BA shall make any amendment(s) to PHI in a Designated Record Set that the CE directs or agrees to, pursuant to 45 C.F.R. section 164.526, or take other measures as necessary to satisfy CE's obligations under 45 C.F.R. section 164.526, in the time and manner designated by the CE.

8. Access to Records

   BA shall make internal practices, books, and records, including policies and procedures, relating to the use, access and disclosure of PHI received from, or created or received by BA on behalf of, CE available to the Secretary of HHS, in a time and manner designated by the Secretary, for purposes of the Secretary determining CE's compliance with the Privacy Rule and Security Rule and patient confidentiality regulations. Any documentation provided to the Secretary shall also be provided to the CE upon request.

9. Accounting for Disclosures

   BA, its agents and subcontractors shall document disclosures of PHI and information related to such disclosures as required by HIPAA. This requirement does not apply to disclosures made for purposes of TPO. BA shall provide an accounting of disclosures to CE or an Individual, in the time and manner designated by the CE. BA agrees to implement a process that allows for an accounting to be collected and maintained by BA and its agents or subcontractors for at least six (6) years prior to the request. 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 PHI and, if known, the address of the entity or person; (iii) a brief description of PHI 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.

10. Termination

    CE may immediately terminate this agreement, and any related agreements, if CE determines that BA has breached a material term of this agreement. CE may, at its sole discretion, provide BA an opportunity to cure the breach or end the violation within the time specified by the CE.

11. Return of PHI

    Upon termination of this Agreement, BA shall return all PHI required to be retained by the BA or its subcontractors, employees or agents on behalf of the CE. In the event the BA determines that returning the PHI is not feasible, the BA shall provide the CE with written notification of the conditions that make return not feasible. Additionally, the BA must follow established policies and procedures to ensure PHI is safeguarded and disposed of adequately in accordance with 45 C.F.R. section 164.310, and must submit to the CE a certification of destruction of PHI. For destruction of ePHI, the National Institute of Standards and Technology (NIST) guidelines must be followed. BA further agrees to extend any and all protections, limitations, and restrictions contained in this Agreement, to any PHI retained by BA or its subcontractors, employees or agents after the termination of this Agreement, and to limit any further use, access or disclosures.

12. Breach by the CE

    Pursuant to 42 U.S.C. section 17934, subdivision (b), if the BA is aware of any activity or practice by the CE that constitutes a material Breach or violation of the CE's obligations under this Agreement, the BA must take reasonable steps to address the Breach and/or end eliminate the continued violation, if the BA has the capability of mitigating said violation. If the BA is unsuccessful in eliminating the violation and the CE continues with non-compliant activity, the BA must terminate the Agreement (if feasible) and report the violation to the Secretary of HHS.

13. Mitigation

BA shall have procedures in place to mitigate, to the extent practicable, any harmful effect that is known to BA of a use, access or disclosure of PHI by BA, its agents or subcontractors in violation of the requirements of this Agreement.

14. Costs Associated to Breach

    BA shall be responsible for reasonable costs associated with a Breach. Costs shall be based upon the required notification type as deemed appropriate and necessary by the CE and shall not be reimbursable under the Agreement at any time. CE shall determine the method to invoice the BA for said costs. Costs shall incur at the current rates and may include, but are not limited to the following:

    - Postage;
    - Alternative means of notice;
    - Media notification; and
    - Credit monitoring services.

15. Direct Liability

    BA may be held directly liable under HIPAA for impermissible uses and disclosures of PHI; failure to provide breach notification to CE; failure to provide access to a copy of ePHI to CE or individual; failure to disclose PHI to the Secretary of HHS when investigating BA's compliance with HIPAA; failure to provide an accounting of disclosures; and, failure to enter into a business associate agreement with subcontractors.

16. Indemnification

    BA agrees to indemnify, defend and hold harmless CE and its authorized officers, employees, agents and volunteers from any and all claims, actions, losses, damages, penalties, injuries, costs and expenses (including costs for reasonable attorney fees) that are caused by or result from the acts or omissions of BA, its officers, employees, agents and subcontractors, with respect to the use, access, maintenance or disclosure of CE's PHI, including without limitation, any Breach of PHI or any expenses incurred by CE in providing required Breach notifications.

17. Judicial or Administrative Proceedings

    CE may terminate the Contract, effective immediately, if (i) BA is named as a defendant in a criminal proceeding for a violation of HIPAA, the HITECH Act, the Privacy Rule, Security Rule or other security or privacy laws or (ii) a finding or stipulation is made in any administrative or civil proceeding in which the BA has been joined that the BA has violated any standard or requirement of HIPAA, the HITECH Act, the Privacy Rule, Security Rule or other security or privacy laws.

18. Insurance

    In addition to any general and/or professional liability insurance coverage required of BA under the Contract for services, BA shall provide appropriate liability insurance coverage during the term of this Agreement to cover any and all claims, causes of action, and demands whatsoever made for loss, damage, or injury to any person arising from the breach of the security, privacy, or confidentiality obligations of BA, its agents or employees, under this Agreement and under HIPAA 45 C.F.R. Parts 160 and 164, Subparts A and E.

19. Assistance in Litigation or Administrative Proceedings

    BA shall make itself, and any subcontractors, employees, or agents assisting BA in the performance of its obligations under the Agreement, 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 BA or its subcontractor, employee or agent is a named adverse party.

C. Obligations of CE

1. CE shall notify BA of any of the following, to the extent that such may affect BA's use, access, maintenance or disclosure of PHI:

   i. Any limitation(s) in CE's notice of privacy practices in accordance with 45 C.F.R. section 164.520.

   ii. Any changes in, or revocation of, permission by an individual to use, access or disclose PHI.

   iii. Any restriction to the use, access or disclosure of PHI that CE has agreed to in accordance with 45 C.F.R. section 164.522.

D. General Provisions

1. Remedies

   BA agrees that CE shall be entitled to seek immediate injunctive relief as well as to exercise all other rights and remedies which CE may have at law or in equity in the event of an unauthorized use, access or disclosure of PHI by BA or any agent or subcontractor of BA that received PHI from BA.

2. Ownership

   The PHI shall be and remain the property of the CE. BA agrees that it acquires no title or rights to the PHI.

3. Regulatory References

   A reference in this Agreement to a section in the Privacy Rule and Security Rule and patient confidentiality regulations means the section as in effect or as amended.

4. No Third-Party Beneficiaries

   Nothing express or implied in the Contract or this Agreement is intended to confer, nor shall anything herein confer, upon any person other than CE, BA and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

5. Amendment

   The parties acknowledge that state and federal laws related to privacy and security of PHI are rapidly evolving and that amendment of the Contract or this Agreement may be required to ensure compliance with such developments. The parties shall negotiate in good faith to amend this Agreement when and as necessary to comply with applicable laws. If either party does not agree to so amend this Agreement within 30 days after receiving a request for amendment from the other, either party may terminate the Agreement upon written notice. To the extent an amendment to this Agreement is required by law and this Agreement has not been so amended to comply with the applicable law in a timely manner, the amendment required by law shall be deemed to be incorporated into this Agreement automatically and without further action required by either of the parties. Subject to the foregoing, this Agreement may not be modified, nor shall any provision hereof be waived or amended, except in a writing duly signed and agreed to by BA and CE.

6. Interpretation

   Any ambiguity in this Agreement shall be resolved to permit CE to comply with the Privacy and Security Rules, the HITECH Act, and all applicable patient confidentiality regulations.

7. Compliance with State Law

   In addition to HIPAA and all applicable HIPAA Regulations, BA acknowledges that BA and CE may have confidentiality and privacy obligations under State law, including, but not limited to, the California Confidentiality of Medical Information Act (Cal. Civil Code §56, et seq. ("CMIA")). If any provisions of this Agreement or HIPAA Regulations or the HITECH Act conflict with CMIA or any other California State law regarding the degree of protection provided for PHI and patient medical records, then BA shall comply with the more restrictive requirements.

8. Survival

   The respective rights and obligations and rights of CE and BA relating to protecting the confidentiality or a patient's PHI shall survive the termination of the Contract or this Agreement.

ATTACHMENT B
APPENDIX B – "BEST AND FINAL OFFER"

The County requests that proposers submit this revised Pricing Sheet as a Best and Final Offer. This revised Pricing Sheets seeks one combined total amount for the performance of the Category 1 and Category 2 mandatory activities for all eleven Health Care Component departments. In addition, the County seeks the best and final offer for Categories 3 and 4 for all HCC departments, delineated separately.

The County provides the following clarification in requesting submission of the Best and Final Offer:

a) For each department, all vulnerability scans are to be performed from a single-location (i.e., Data Center).
   1) Sampling methodology required for departments with IPs greater than one-thousand (1,000).
   2) Vulnerability scan type is credentialed and preferred; use of non-credentialed scans require notation.
b) For each department, all internal penetration tests are to be performed from a single-location (i.e., Data Center).
c) Healthcare related devices/equipment are not included in the vulnerability scan process.
d) A health-check follow-up is included for each department that must occur twelve (12) months after department assessment.

CATEGORIES 1 AND 2:

Combined cost for completion of Category 1 and Category 2 tasks as defined in the RFP for all eleven departments within the Health Care Component. The expectation is that one assessment will be completed for each department over the course of one year (or if an extended period is necessary please indicate). Individual departments that require assessments to be completed annually, will negotiate directly with the awarded contractor for such additional assessments.

Total Amount for 11 HCC Departments $ 500,000

Time Period if greater than one year: _____

CATEGORIES 3 AND 4

The cost for the completion of Categories 3 and 4 separately listed for each department.

Category 3:

a. Information Services Department $ 10k
b. Arrowhead Regional Medical Center $ 15k
c. Behavioral Health $ 5k
d. Public Health $ 5k
e. Aging and Adult Services $ 5k
f. Auditor-Controller/Treasurer/Tax Collector $ 5k
g. Board of Supervisors $ 5k
h. County Administrative Office $ 5k

i. County Counsel $ 5k

j. Human Resources – Emp. Benefits Division $ 5k

k. Risk Management $ 5k

Category 4:

a. Information Services Department $ 5k

b. Arrowhead Regional Medical Center $ 10k

c. Behavioral Health $ 2k

d. Public Health $ 2k

e. Aging and Adult Services $ 2k

f. Auditor-Controller/Treasurer/Tax Collector $ 2k

g. Board of Supervisors $ 2k

h. County Administrative Office $ 2k

j. County Counsel $ 2k

j. Human Resources – Emp. Benefits Division $ 2k

k. Risk Management $ 2k

EXHIBIT A – HCC Department Locations and Devices

The chart below identifies specific locations that are part of the services requested for this engagement.

DEPARTMENT	LOCATION / FACILITY	TOTAL NUMBER of DEVICES (or IPs) to be scanned (estimated)	TOTAL NUMBER of EMPLOYEES (HIPAA focused) (Fiscal Year 2018-19)
Information Services	Data Center 670 East Gilbert Street San Bernardino CA 92415	CAO = 1 Counsel = 1 DPH = 68	360
ARMC	Arrowhead Regional Medical Center (ARMC) 400 North Pepper Avenue Colton CA 92324	1835 (1500 desktops)	5,200
Behavioral Health	303 East Vanderbilt Way San Bernardino CA 92415	300	589
	658 Brier Street San Bernardino, CA 92415	200	
Public Health	Carmack Medical Therapy Unit 4777 State Street San Bernardino CA 92415	21	600
	Etiwanda Medical Therapy Unit 12860 Banyan Street Rancho Cucamonga CA	14	
	Hesperia Health Center 16453 Bear Valley Road Hesperia CA 92345	156	
	Ontario Health Center 150 East Holt Boulevard Ontario CA 91761	332	
Aging & Adult Services	784 E. Hospitality Lane San Bernardino CA 92415	11	11
Auditor-Controller/ Treasurer/Tax Collector	268 W. Hospitality Lane, 4th Fl San Bernardino CA 92415	2	120
Board of Supervisors	385 N. Arrowhead Ave., 5th Fl San Bernardino CA 92415	ISD	10
County Administrative Office	385 N. Arrowhead Ave., 5th Fl San Bernardino CA 92415	ISD	12
County Counsel	385 N. Arrowhead Ave., 4th Fl San Bernardino CA 92415	ISD	96
Human Resources – Employee Benefits & Services Division	157 W Fifth Street, 1st Fl San Bernardino CA 92415	12	35
Risk Management	222 W. Hospitality Lane, 3rd Fl San Bernardino CA 92415	21 (1 server)	67

EXHIBIT B - Risk Levels

The following chart was obtained from the U.S. Department of Health and Human Services, Center for Medicare and Medicaid Services (CMS). It defines risk levels in terms of confidentiality, integrity, and availability that may result in a compromise of the system or process; and the data it handles. Tables 2 and 3 are used to define and identify what is described in Table 1. Table 1 shall be used to identify the Impact Severity for a particular activity, procedure, or process as it relates to the HIPAA Security rule.

Table 1

Likelihood of Occurrence	Impact Severity					
	Insignificant	**Minor**	**Significant**	**Damaging**	**Serious**	**Critical**
Negligible	Low	Low	Low	Low	Low	Low
Very Low	Low	Low	Low	Low	Moderate	Moderate
Low	Low	Low	Moderate	Moderate	High	High
Medium	Low	Low	Moderate	High	High	High
High	Low	Moderate	High	High	High	High
Very High	Low	Moderate	High	High	High	High
Extreme	Low	Moderate	High	High	High	High

Table 2

Likelihood of Occurrence Description	
Negligible	Unlikely to occur.
Very Low	Likely to occur two/three times every five years.
Low	Likely to occur one every year or less.
Medium	Likely to occur once every six months or less.
High	Likely to occur once per month or less.
Very High	Likely to occur multiple times per month.
Extreme	Likely to occur multiple times per day.

Table 3

Impact Severity Levels Description	
Insignificant	Will have almost no impact if threat is realized, exploiting a vulnerability.
Minor	Will have some minor effect on the system. It will require minimal effort to repair or reconfigure the system.
Significant	Will result in some tangible harm, albeit negligible and perhaps only noted by a few individuals or agencies. May cause political embarrassment. Will require some expenditure of resources to repair.
Damaging	May cause damage to the reputation of system management, and/or notable loss of confidence in the system's resources or services. It will require expenditure of significant resources to repair.
Serious	May cause considerable system outage, and/or loss of connected customers or business confidence. May result in the compromise of a large amount of Government information or services.
Critical	May cause an extended outage of a system or a location to be permanently closed, causing operations to resume in a Hot Site environment. May result in complete compromise of Government agencies' information or services.

EXHIBIT C – Consultant's Organizational Chart

Organizational Chart