Natividad MEDICAL CENTER

COUNTY OF MONTEREY AGREEMENT FOR SERVICES (MORE THAN $100,000)

This Agreement for Services (hereinafter "Agreement") is made by and between the County of Monterey, a political subdivision of the State of California (hereinafter, "the County"), on behalf of Natividad Medical Center ("NMC"), a general acute care teaching hospital wholly owned and operated by the County, and CynergisTek, Inc. (hereinafter "CONTRACTOR").

In consideration of the mutual covenants and conditions set forth in this Agreement, the parties agree as follows:

1. **GENERAL DESCRIPTION OF SERVICES TO BE PROVIDED.** NMC hereby engages CONTRACTOR to perform, and CONTRACTOR hereby agrees to perform, the services described in **Exhibit A** in conformity with the terms of the Agreement. The services are generally described as follows: Provide Information Security Services to include an IT Security Assessment and related deliverables and Consulting services for NMC.

2. **PAYMENTS BY NMC.** NMC shall pay the CONTRACTOR in accordance with the payment provisions set forth in **Exhibit A**, subject to the limitations set forth in this Agreement. The total amount payable by NMC to CONTRACTOR under this Agreement shall not exceed the sum of $457,200.00.

3. **TERM OF AGREEMENT.**

   3.1. The term of this Agreement is from October 1, 2016 through September 30, 2019 unless sooner terminated pursuant to the terms of this Agreement. This Agreement is of no force or effect until signed by both CONTRACTOR and NMC and with NMC signing last and CONTRACTOR may not commence work before NMC signs this Agreement.

MGM 3.2. ~~NMC reserves the right to cancel this Agreement, or an extension of this Agreement, without cause, with a thirty (30) day written notice, or with cause immediately.~~

4. **ADDITIONAL PROVISIONS/EXHIBITS.** The following attached exhibits are incorporated herein by reference and constitute a part of this Agreement:

   Exhibit A: Scope of Services/Payment Provisions
   Exhibit B: Business Associates Agreement
   Addendum 1: Addendum to Agreement Terms and Conditions

5. **PERFORMANCE STANDARDS.**

   5.1. CONTRACTOR warrants that CONTRACTOR and Contractor's agents, employees, and subcontractors performing services under this Agreement are specially trained, experienced, competent, and appropriately licensed to perform the work and deliver the services required

under this Agreement and are not employees of NMC, or immediate family of an employee of NMC.

5.2. CONTRACTOR, its agents, employees, and subcontractors shall perform all work in a safe and skillful manner and in compliance with all applicable laws and regulations. All work performed under this Agreement that is required by law to be performed or supervised by licensed personnel shall be performed in accordance with such licensing requirements.

5.3. CONTRACTOR shall furnish, at its own expense, all materials, equipment, and personnel necessary to carry out the terms of this Agreement, except as otherwise specified in this Agreement. CONTRACTOR shall not use NMC premises, property (including equipment, instruments, or supplies) or personnel for any purpose other than in the performance of its obligations under this Agreement.

6. PAYMENT CONDITIONS.

6.1. Prices shall remain firm for the initial term of the Agreement and, thereafter, may be adjusted annually as provide in this paragraph. NMC does not guarantee any minimum or maximum amount of dollars to be spent under this Agreement.

6.2. Negotiations for rate changes shall be commenced, by CONTRACTOR, a minimum of ninety (90) days prior to the expiration of the Agreement. Rate changes are not binding unless mutually agreed upon in writing by the County (NMC) and the CONTRACTOR.

6.3. CONTRACTOR shall not receive reimbursement for travel expenses unless set forth in this Agreement, and then only in accordance with any applicable County policies.

6.4. Invoice amounts shall be billed directly to the ordering department.

6.5. CONTRACTOR shall submit such invoice periodically or at the completion of services, but in any event, not later than 30 days after completion of services. The invoice shall set forth the amounts claimed by CONTRACTOR for the previous period, together with an itemized basis for the amounts claimed, and such other information pertinent to the invoice. NMC shall certify the invoice, either in the requested amount or in such other amount as NMC approves in conformity with this Agreement, and shall promptly submit such invoice to the County Auditor-Controller for payment. The County Auditor-Controller shall pay the amount certified within 30 days of receiving the certified invoice.

7. TERMINATION.

7.1. During the term of this Agreement, NMC may terminate the Agreement for any reason by giving written notice of termination to the CONTRACTOR at least thirty (30) days prior to the effective date of termination. Such notice shall set forth the effective date of termination. In the event of such termination, the amount payable under this Agreement shall be reduced in proportion to the services provided prior to the date of termination.

7.2. NMC may cancel and terminate this Agreement for good cause effective immediately upon written notice to Contractor. "Good cause" includes the failure of CONTRACTOR to perform the required services at the time and in the manner provided under this Agreement. If

NMC terminates this Agreement for good cause, NMC may be relieved of the payment of any consideration to Contractor, and NMC may proceed with the work in any manner, which NMC deems proper. The cost to NMC shall be deducted from any sum due the CONTRACTOR under this Agreement.

7.3 NMC's payments to CONTRACTOR under this Agreement are funded by local, state and federal governments. If funds from local, state and federal sources are not obtained and continued at a level sufficient to allow for NMC's purchase of the indicated quantity of services, then NMC may give written notice of this fact to CONTRACTOR, and the obligations of the parties under this Agreement shall terminate immediately, or on such date thereafter, as the County may specify in its notice, unless in the meanwhile the parties enter into a written amendment modifying this Agreement.

8. INDEMNIFICATION.

8.1 ~~CONTRACTOR shall indemnify, defend, and hold harmless the County of Monterey (hereinafter "County"), its officers, agents and employees from any and all claims, liability and losses whatsoever (including damages to property and injuries to or death of persons, court costs, and reasonable attorneys' fees) occurring or resulting to any and all persons, firms or corporations furnishing or supplying work, services, materials, or supplies in connection with the performance of this Agreement, and from any and all claims, liabilities, and losses occurring or resulting to any person, firm, or corporation for damage, injury, or death arising out of or connected with the CONTRACTOR's performance of this Agreement, unless such claims, liabilities, or losses arise out of the sole negligence or willful misconduct of County. "CONTRACTOR's performance" includes CONTRACTOR's action or inaction and the action or inaction of CONTRACTOR's officers, employees, agents and subcontractors.~~

MGM

9. INSURANCE.

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

This verification of coverage shall be sent to NMC's Contracts/Purchasing Department, unless otherwise directed. The CONTRACTOR shall not receive a "Notice to Proceed" with the work under this Agreement until it has obtained all insurance required and NMC has approved such insurance. This approval of insurance shall neither relieve nor decrease the liability of CONTRACTOR.

9.2 Qualifying Insurers: All coverage's, except surety, shall be issued by companies which hold a current policy holder's alphabetic and financial size category rating of not less than A-VII, according to the current Best's Key Rating Guide or a company of equal financial stability that is approved by NMC's Contracts/Purchasing Director.

9.3 Insurance Coverage Requirements: Without limiting CONTRACTOR's duty to indemnify, CONTRACTOR shall maintain in effect throughout the term of this Agreement a policy or policies of insurance with the following minimum limits of liability:

Commercial general liability insurance, including but not limited to premises and operations, including coverage for Bodily Injury and Property Damage, Personal Injury, Contractual Liability, Broad form Property Damage, Independent Contractors, Products and Completed Operations, with a combined single limit for Bodily Injury and Property Damage of not less than $1,000,000 per occurrence.

☐ Exemption/Modification (Justification attached; subject to approval).

Business automobile liability insurance, covering all motor vehicles, including owned, leased, non-owned, and hired vehicles, used in providing services under this Agreement, with a combined single limit for Bodily Injury and Property Damage of not less than $1,000,000 per occurrence.

☐ Exemption/Modification (Justification attached; subject to approval).

Workers' Compensation Insurance, If CONTRACTOR employs others in the performance of this Agreement, in accordance with California Labor Code section 3700 and with Employer's Liability limits not less than $1,000,000 each person, $1,000,000 each accident and $1,000,000 each disease.

☐ Exemption/Modification (Justification attached; subject to approval).

Professional liability insurance, if required for the professional services being provided, (e.g., those persons authorized by a license to engage in a business or profession regulated by the California Business and Professions Code), in the amount of not less than $1,000,000 per claim and $2,000,000 in the aggregate, to cover liability for malpractice or errors or omissions made in the course of rendering professional services. If professional liability insurance is written on a "claims-made" basis rather than an occurrence basis, the CONTRACTOR shall, upon the expiration or earlier termination of this Agreement, obtain extended reporting coverage ("tail coverage") with the same liability limits. Any such tail coverage shall continue for at least three years following the expiration or earlier termination of this Agreement.

☐ Exemption/Modification (Justification attached; subject to approval).

9.4 Other Requirements:

All insurance required by this Agreement shall be with a company acceptable to NMC and issued and executed by an admitted insurer authorized to transact insurance business in the State of California. Unless otherwise specified by this Agreement, all such insurance shall be written on an occurrence basis, or, if the policy is not written on an occurrence basis, such policy with the coverage required herein shall continue in effect for a period of three years following the date CONTRACTOR completes its performance of services under this Agreement.

Each liability policy shall provide that NMC shall be given notice in writing at least thirty days in advance of any endorsed reduction in coverage or limit, cancellation, or intended non-renewal thereof. Each policy shall provide coverage for CONTRACTOR and additional insured with respect to claims arising from each subcontractor, if any, performing work under this Agreement, or be accompanied by a certificate of insurance from each subcontractor showing each subcontractor has identical insurance coverage to the above requirements.

Commercial general liability and automobile liability policies shall provide an endorsement naming the County of Monterey, its officers, agents, and employees as Additional insureds with respect to liability arising out of the Contractor's work, including ongoing and completed operations, **and shall further provide that such insurance is primary insurance to any insurance or self-insurance maintained by the County and that the insurance of the Additional Insureds shall not be called upon to contribute to a loss covered by the Contractor's insurance.** The required endorsement from for Commercial General Liability Additional Insured is ISO Form CG 20 10 11-85 or CG 20 10 10 01 in tandem with CG 20 37 10 01 (2000). The required endorsement from for Automobile Additional Insured Endorsement is ISO Form CA 20 48 02 99.

Prior to the execution of this Agreement by NMC, CONTRACTOR shall file certificates of insurance with NMC's Contracts/Purchasing Department, showing that the CONTRACTOR has in effect the insurance required by this Agreement. The CONTRACTOR shall file a new or amended certificate of insurance within five (5) calendar days after any change is made in any insurance policy, which would alter the information on the certificate then on file. Acceptance or approval of insurance shall in no way modify or change the indemnification clause in this Agreement, which shall continue in full force and effect.

CONTRACTOR shall at all times during the term of this Agreement maintain in force the insurance coverage required under this Agreement and shall send, without demand by NMC, annual certificates to NMC's Contracts/Purchasing Department. If the certificate is not received by the expiration date, NMC shall notify CONTRACTOR and CONTRACTOR shall have five calendar days to send in the certificate, evidencing no lapse in coverage during the interim. Failure by CONTRACTOR to maintain such insurance is a default of this Agreement, which entitles NMC, at its sole discretion, to terminate the Agreement immediately.

10. RECORDS AND CONFIDENTIALITY.

10.1 Confidentiality. CONTRACTOR and its officers, employees, agents and subcontractors shall comply with any and all federal, state, and local laws, which provide for the confidentiality of records and other information. CONTRACTOR shall not disclose any confidential records or other confidential information received from NMC or prepared in connection with the performance of this Agreement, unless NMC specifically permits CONTRACTOR to disclose such records or information. CONTRACTOR shall promptly transmit to NMC any and all requests for disclosure of any such confidential records or information. CONTRACTOR shall not use any confidential information gained by CONTRACTOR in the performance of this Agreement except for the sole purpose of carrying out CONTRACTOR's obligations under this Agreement.

10.2 NMC Records. When this Agreement expires or terminates, CONTRACTOR shall return to NMC any NMC records which CONTRACTOR used or received from NMC to perform services under this Agreement.

10.3 Maintenance of Records. CONTRACTOR shall prepare, maintain, and preserve all reports and records that may be required by federal state, and County rules and regulations related to services performed under this Agreement. CONTRACTOR shall maintain such records for a period of at least three years after receipt of final payment under this Agreement. If any litigation, claim, negotiation, audit exception, or other action relating to this Agreement is pending at the end of the three year period, then CONTRACTOR shall retain said records until such action is resolved.

10.4 Access to and Audit of Records. NMC shall have the right to examine, monitor and audit all records, documents, conditions, and activities of the CONTRACTOR and its subcontractors related to services provided under this Agreement. Pursuant to Government Code section 8546.7, if this Agreement involves the expenditure of public funds in excess or $10,000, the parties to this Agreement may be subject, at the request of NMC or as part of any audit of NMC, to the examination and audit of the State Auditor pertaining to matters connected with the performance of this Agreement for a period of three years after final payment under the Agreement.

10.5 Royalties and Inventions. NMC shall have a royalty-free, exclusive and irrevocable license to reproduce, publish, and use, and authorize other to do so, all original computer programs, writings, sound recordings, pictorial reproductions, drawings, and other works of similar nature produced in the course of or under this Agreement. CONTRACTOR shall not publish any such material without the prior written approval of NMC.

11. **NON-DISCRIMINATION**. During the performance of this Agreement, CONTRACTOR, and its subcontractors, shall not unlawfully discriminate against any person because of race, religious creed, color, sex, national origin, ancestry, physical disability, mental disability, medical condition, marital status, age (over 40), or sexual orientation, either in CONTRACTOR's employment practices or in the furnishing of services to recipients. CONTRACTOR shall ensure that the evaluation and treatment of its employees and applicants for employment and all persons receiving and requesting services are free of such discrimination. CONTRACTOR and any subcontractor shall, in the performance of this Agreement, full comply with all federal, state, and local laws and regulations which prohibit discrimination. The provision of services primarily or exclusively to such target population as may be designated in this Agreement shall not be deemed to be prohibited discrimination.

12. **COMPLIANCE WITH TERMS OF STATE OR FEDERAL GRANT**. If this Agreement has been or will be funded with monies received by NMC pursuant to a contract with the state or federal government in which NMC is the grantee, CONTRACTOR will comply with all the provisions of said contract, and said provisions shall be deemed a part of this Agreement, as though fully set forth herein. Upon request, NMC will deliver a copy of said contract to CONTRACTOR, at no cost to CONTRACTOR.

13. **INDEPENDENT CONTRACTOR.** In the performance of work, duties, and obligations under this Agreement, CONTRACTOR is at all times acting and performing as an independent CONTRACTOR and not as an employee of NMC. No offer or obligation of permanent

employment with NMC or particular County department or agency is intended in any manner, and CONTRACTOR shall not become entitled by virtue of this Agreement to receive from NMC any form of employee benefits including but not limited to sick leave, vacation, retirement benefits, workers' compensation coverage, insurance or disability benefits. CONTRACTOR shall be solely liable for and obligated to pay directly all applicable taxes, including federal and state income taxes and social security, arising out of CONTRACTOR's performance of this Agreement. In connection therewith, CONTRACTOR shall defend, indemnify, and hold NMC and the County of Monterey harmless from any and all liability, which NMC may incur because of CONTRACTOR's failure to pay such taxes.

14. **NOTICES.** Notices required under this Agreement shall be delivered personally or by first-class, postage per-paid mail to NMC and CONTRACTOR's contract administrators at the addresses listed below

NATIVIDAD MEDICAL CENTER:	**CONTRACTOR:**
Natividad Medical Center Attn: Contracts Division 1441Constitution Blvd Salinas, CA. 93906 FAX: 831-757-2592	Business Name: CynergisTek, Inc. Attn: COO Address: 11410 Jollyville Road Suite 2201 City, State, Zip: Austin, TX 78759 FAX: 512 857-0700 Email: operations@cynergistek.com

15. MISCELLANEOUS PROVISIONS.

15.1 Conflict of Interest: CONTRACTOR represents that it presently has no interest and agrees not to acquire any interest during the term of this Agreement, which would directly, or indirectly conflict in any manner or to any degree with the full and complete performance of the professional services required to be rendered under this Agreement.

15.2 Amendment: This Agreement may be amended or modified only by an instrument in writing signed by NMC and the CONTRACTOR.

15.3 Waiver: Any waiver of any terms and conditions of this Agreement must be in writing and signed by NMC and the CONTRACTOR. A waiver of any of the terms and conditions of this Agreement shall not be construed as a waiver of any other terms or conditions in this Agreement.

15.4 Contractor: The term "CONTRACTOR" as used in this Agreement includes CONTRACTOR's officers, agents, and employees acting on CONTRACTOR's behalf in the performance of this Agreement.

15.5 Disputes: CONTRACTOR shall continue to perform under this Agreement during any dispute.

15.6 Assignment and Subcontracting: The CONTRACTOR shall not assign, sell, or otherwise transfer its interest or obligations in this Agreement without the prior written consent of NMC. None of the services covered by this Agreement shall be subcontracted without the prior written approval of NMC. Notwithstanding any such subcontract, CONTRACTOR shall continue to be liable for the performance of all requirements of this Agreement.

15.7 Successors and Assigns: This Agreement and the rights, privileges, duties, and obligations of NMC and CONTRACTOR under this Agreement, to the extent assignable or delegable, shall be binding upon and inure to the benefit of the parties and their respective successors, permitted assigns, and heirs.

15.8 Compliance with Applicable Law: The parties shall comply with all applicable federal, state, and local laws and regulations in performing this Agreement.

15.9 Headings: The headings are for convenience only and shall not be used to interpret the terms of this Agreement.

15.10 Time is of the Essence: Time is of the essence in each and all of the provisions of this Agreement

15.11 Governing Law: This Agreement shall be governed by and interpreted under the laws of the State of California.

15.12 Non-exclusive Agreement: This Agreement is non-exclusive and each of NMC and CONTRACTOR expressly reserves the right to contract with other entities for the same or similar services.

15.13 Construction of Agreement: NMC and CONTRACTOR agree that each party has fully participated in the review and revision of this Agreement and that any rule of construction to the effect that ambiguities are to be resolved against the drafting party shall not apply in the interpretation of this Agreement or any amendment to this Agreement.

15.14 Counterparts: This Agreement may be executed in two or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same Agreement.

15.15 Integration: This Agreement, including the exhibits, represents the entire Agreement between NMC and the CONTRACTOR with respect to the subject matter of this Agreement and shall supersede all prior negotiations representations, or agreements, either written or oral, between NMC and CONTRACTOR as of the effective date of this Agreement, which is the date that NMC signs the Agreement.

15.16 Interpretation of Conflicting Provisions: In the event of any conflict or inconsistency between the provisions of this Agreement and the Provisions of any exhibit or other attachment to this Agreement, the provisions of this Agreement shall prevail and control.

NATIVIDAD MEDICAL CENTER

By: _____
Gary R. Gray, DO, CEO

Date: _____

APPROVED AS TO LEGAL PROVISIONS

By: _____
Monterey County Deputy County Counsel

Date: Sept 23, 2016

APPROVED AS TO FISCAL PROVISIONS

By: _____
Monterey County Deputy Auditor/Controller

Date: 9-23-16

CONTRACTOR

Cynergistek, Inc.
Contractor's Business Name*** (see instructions)

_____
Signature of Chair, President, or Vice-President

Michael H. McMillan, Chairman & CEO
Name and Title

Date: 01-Sep-16

By: _____
(Signature of Secretary, Asst. Secretary, CFO, Treasurer or Asst. Treasurer)

Dr. Michael G. Mathews, President & COO
Name and Title

Date: 01-Sep-16

***__Instructions:__

If CONTRACTOR is a corporation, including limited liability and non-profit corporations, the full legal name of the corporation shall be set forth above together with the signatures of two specified officers (two signatures required).
If CONTRACTOR is a partnership, the name of the partnership shall be set forth above together with the signature of a partner who has authority to execute this Agreement on behalf of the partnership (two signatures required).
If CONTRACTOR is contracting in and individual capacity, the individual shall set forth the name of the business, if any and shall personally sign the Agreement (one signature required).

CYNERGISTEK

11410 Jollyville Rd
Suite 2201
Austin, Texas 78759
http://cynergistek.com
info@cynergistek.com
512.402.8550 Phone
512.857.0700 FAX

EXHIBIT A

Scope of Services/Payment Provisions

Prepared For:

Natividad Medical Center

Contact: Ari Entin
Email: EntinA@Natividad.com
Phone: 831.783.2564

1. Scope and Approach

The following sub-sections document each of the elements included in this engagement including the scope for each element as well as a brief description of what each component is and our approach for completing each of them.

1.1. External Security Assessment

Scope

The external security assessment scope includes up to 32 IP connected assets visible from the Internet and all services answering on those assets.

External technical testing will be performed quarterly (4x per year) during the term of this engagement (one per year as part of the annual assessment).

Approach

The purpose of the External Security Assessment is to evaluate the overall security posture of the enterprise from the perspective of an anonymous source on the Internet. Our methodology starts with a process called "Fingerprinting" during which time we review public sources of information (such as the network registrars, DNS servers, email servers, routing tables, public special interest groups, etc.) to evaluate what potential information is available for the anonymous attacker to gather as base information to start an attack. The next phase of the review is to perform technical testing to gather data on open ports and vulnerabilities. The final phase is to perform analysis and reporting on the data collected. Our summary of findings and recommendations includes root cause analysis of the data collected during the engagement and offers the management team a project-based, prioritized view of remediation steps.

1.2. Architecture Assessment

Scope

The Architecture Assessment includes detailed analysis of up to 5 network architecture diagrams, 12 router, 12 switch, and 6 firewall configuration files and interviews with key stakeholders in IS/IT.

An architecture assessment will be performed once per year as part of the annual assessment during the term of this engagement.

Approach

The Architecture Assessment is the foundation upon which the technical evaluation of an enterprise security program is based. The goal is to evaluate, from a technical perspective, the maturity of various components of an enterprise's information security program. The process starts with requests for network diagrams and device configurations (routers, switches, firewalls, etc.) to evaluate against common security holes, misconfigurations, and vulnerabilities associated with network design and configuration management practices. The balance of the process mirrors the Information Security Program Assessment, but from a technical perspective rather than a process/procedure perspective. We interview stakeholders to evaluate security controls around the following areas from a technical perspective as they relate to the risk management process overall:

- Perimeter Security
- Network Segmentation, Design, and Security
- Host Security

- Application, Patch, and Configuration Management
- Tactical Implementation of Administrative Security

The data collected, our findings and recommendations, and other output from the architecture assessment feeds vital information directly into the enterprise risk analysis process.

1.3. INTERNAL SECURITY ASSESSMENT

Scope

The internal security assessment scope includes up to 512 IP connected assets and all services answering on those assets. Typically we recommend separating into asset groups of like kind (i.e. network gear, servers, printers, workstations, etc.) so that we have more granular control over timing, asset exposure at any given time during scanning activities, and visibility into the scanning process to help inform potential trouble tickets associated with scanning activities.

Internal technical testing will be performed twice (2x) per year during the term of this engagement (one per year as part of the annual assessment).

Approach

The purpose of the Internal Security Assessment is to evaluate the overall security posture of the enterprise against potential attacks from "insiders" or other trusted parties. In conjunction with the architecture assessment as a first step, CynergisTek will perform technical testing to gather data on open ports and vulnerabilities across the different groups of assets provided to us. With the data we collect during this phase and in conjunction with information gathered during the architecture assessment, we then perform extensive root cause analysis prior to compiling a summary report of findings. The summary of findings and recommendations are presented in addition to the detailed raw reporting from the vulnerability testing. The vulnerability testing reports provide comprehensive recommendations for addressing all issues discovered while the summary report of findings identifies gaps in program components that, when viewed as remediation projects, address whole groups of vulnerabilities at a time by virtue of process improvements rather than one-off remediation activities.

1.4. WIRELESS LAN SECURITY VALIDATION

Scope

The Wireless LAN Security Validation includes one physical space on one campus measuring no more than 12,500 square feet in area.

A wireless LAN assessment will be performed once per year as part of the annual assessment during the term of this engagement.

Approach

The Wireless LAN Security Validation is designed to serve as an audit-style verification of information collected during the Architecture Assessment interview process as it relates to implemented security controls on the wireless LAN compared to industry best practices. Our goal is to identify and document wireless access points that will grant access to a particular network and any of the specifics associated with that network. During the course of conducting the Wireless LAN Security Validation, CynergisTek will look for and enumerate access points that grant access (either through encrypted or non-encrypted channels), what frequency/channel, signal strength, associated SSID, authentication requirements, and access control specifics associated with each. The data collected during this portion of the engagement feeds into an overall risk analysis and risk management process. Any relevant findings will be provided against current best practices in deploying wireless LAN technology.

1.5. Information Security Program Assessment

Scope

The Information Security Program Assessment will be conducted at a single physical campus for an organization whose policies and procedures are centralized across the organization. The assessment will be against The NIST 800-53 Controls using the HIPAA Security Rule and the HITECH Act.

The information security program assessment will be performed once per year as part of the annual assessment during the term of this engagement.

Approach

The goal of the Information Security Program Assessment is to evaluate the organization's administrative controls governing the information security program as a whole. CynergisTek will conduct a thorough review of information security policies and procedures, interview key stakeholders, and conduct physical walkthroughs as part of the data collection phase. A sample interview schedule including topics/focus, approximate durations, and target attendees is included as an addendum to this proposal. As a matter of course, we strive to include a disciplined "show me" approach to establish the crucial demonstration of compliance as is typical of sanctioned audits by OCR. The output of this effort is a comprehensive report of findings that clearly articulates the compliance status of the organization for each element of the selected compliance framework (identified in the scope section above) as compliant, non-compliant, or not applicable. As a value add, we also use the COBIT maturity model to rank the organization's maturity for each element of the selected compliance framework.

1.6. Risk Analysis

Scope

The scope of the Risk Analysis includes the facilities and information assets identified within the ISPA section of this proposal (including any additional facility visits that might be identified in Appendix A).

A risk analysis will be performed once per year as part of the annual assessment during the term of this engagement.

Approach

CynergisTek will facilitate an interactive risk analysis working session with key stakeholders. The goal of the working session is to introduce the team to the key elements of risk analysis. CynergisTek's philosophy is that risk management and risk analysis are continuous requirements of an effective information security program operating in a dynamic threat environment. Our approach is broken into nine steps that correspond and are consistent with the NIST SP 800-30 methodology and the Office for Civil Rights HIPAA Guidance of July, 2010 as follows:

- System Characterization
- Threat Identification
- Vulnerability Identification
- Control Analysis
- Likelihood Determination
- Impact Analysis
- Risk Determination
- Controls Recommendations
- Results Documentation

The risk analysis process is a combination of objective quantification of threats, vulnerabilities and controls and the likelihood and potential impacts of risk events occurring that could affect system and data integrity or compliance. HIPAA and HITECH require an enterprise level evaluation of reasonable risks to the confidentiality, integrity and availability of systems containing electronic protected health information. CynergisTek's process involves key stake holders in an interactive working session following the steps enumerated above to develop a concise risk profile. The analysis and findings are captured in a workbook that supports ongoing remediation and compliance. Below is a specific breakdown of the elements of the Risk Analysis process:

System Characterization

The first step of the risk analysis process is to define the focus and scope. Information security related risks in the scope of this engagement will be collected through the use of:

- General Staff Surveys
- Onsite Interviews
- Document Reviews
- Automated Scanning Tools

At the conclusion of the first step, the applications being assessed will be characterized, a good picture of the application environment will be created and the boundary for the assessment will be defined.

Threat Identification

For the threat identification process, the goal is to identify potential threats that could reasonably be expected to occur. Historical events and data will be used to identify potential threats specific to the organization. Threats are presented in four basic forms:

- Human Intentional - People doing things on purpose such as criminal acts
- Human Unintentional - People doing things by accident such as user error
- Natural Environmental - Acts of nature such as lightning or a tornado
- Manmade Environmental - Issues such as a power surge or hardware failure

All potential threats will be identified and documented across the four threat categories. Completion of this step provided a list of threats that could exploit potential vulnerabilities.

Vulnerability Identification

The goal of this step is to identify where potential weaknesses existed that could be exploited by the potential threats. Vulnerabilities will be previously identified during the information security assessment and discussed.

Management, operational and technical issues will be considered. The vulnerabilities will be paired with threats to identify plausible risk scenarios for further analysis. At the conclusion of this step, a list of vulnerabilities will be established that could be exploited by potential threat sources.

Control Analysis

During this step of the process, the goal is to determine the security controls in place, or are planned for implementation, that can contribute to mitigating or managing the vulnerabilities identified from the previous steps. Control categories considered included:

- Technical Controls - safeguards incorporated into computer hardware and software or log management technologies
- Nontechnical Controls - management and operational controls such as policies, procedures, personnel, physical or environmental

For planned controls, the estimated period for implementation will be considered based on resource allocation and funding requirements.

Likelihood Determination

The goal of this step is to determine the likelihood or probability of something undesirable occurring based on a credible threat and an exploitable vulnerability. The exercise considers analysis of the capability and complexity of the threat and the absence of controls or countermeasures to deter an attack or event.

Impact Analysis

The goal is to assess the potential impact to the confidentiality, integrity or availability of data due to a successful attack or event. The impact level will be determined by identifying a negative impact to an inherent ability to operate effectively. Areas potentially impacted include patient safety, loss of reputation, financial loss, data loss, outages or unavailability issues and regulatory noncompliance.

Risk Determination

The goal of this step is to determine the level of risk presented by the potential threats and identified vulnerabilities by assessing the:

- Likelihood of a given threat capable of or motivated to exploit a particular vulnerability or set of vulnerabilities
- Magnitude of potential impacts should a threat exploit a vulnerability
- Adequacy of planned or existing security controls for reducing the risk

Control Recommendations

During this step of the process, the goal is to recommend controls and solutions to mitigate or reduce the risk to an acceptable level. Controls are discussed and listed that could mitigate or minimize the identified risks as appropriate for the applications. Factors considered in the recommendations included:

- Effectiveness of options
- Legislation and regulation
- Organizational policy
- Operational impact

1.7. MEANINGFUL USE EHR SECURITY CONTROLS ASSESSMENT

Scope

The Meaningful Use EHR Technical Security Controls Assessment scope includes up to one (1) electronic health records.

A meaningful use assessment will be performed once per year as part of the annual assessment during the term of this engagement.

Approach

Stage 1 Meaningful Use states that you must "protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities." The measure requires you to "conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of your risk management process."

Stage 2 Meaningful Use reinforces the requirement for organizations to protect electronic health information created or maintained by a Certified EHR Technology (CEHRT) through the implementation of appropriate technical capabilities requiring organizations to conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data stored in a CEHRT in accordance with requirements under 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306 (d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the provider's risk management process for eligible hospitals. A new review must occur during each subsequent reporting period.

CynergisTek's Meaningful Use EHR Technical Security Controls Assessment, in conjunction with a Risk Assessment, will provide you with a deliverable you can use for your attestation process. To gather data for the assessment CynergisTek will conduct interviews and working sessions with key stakeholders as part of an independent verification and validation of each of the privacy and security controls associated with the certified EHR necessary to demonstrate meaningful use. Interviews and working sessions will focus on the demonstration of compliance that each functionality exists, is enabled, performs properly, and that there is a documented process around it to ensure its use.

1.8. Advisory Services

Scope

During the term of this engagement, CynergisTek's staff will be readily available to address questions, concerns, and advice covering the areas of technology, program development and maintenance, and regulatory compliance matters. Requests will be acknowledged and expectations for an answer set within the first business day after the question/query is received. Our entire staff, from the executive team down is made available to address these questions and the answers that are provided will often span the expertise of the entire organization as we discuss the nature and specifics of the question internally before we post a response.

Approach

Requests for advisory services can either be posted to TekTrak, our project management portal and should minimally notify our operations coordinator and the lead consultant on the engagement or can be sent directly via email to advisory@cynergistek.com to establish a request through our ticketing system. All requests will be acknowledged within one business day of being posted, but many times within minutes of the initial posting. There are no limits set around the nature or frequency of use of the advisory service during the term of this engagement. If, in our view, the request launches a new project, we will advise as part of our response and discuss the scope and approach to properly budget and set expectations for a new project.

1.9. Phishing Assessment

Scope

CynergisTek will perform up to four quarterly custom phishing email campaigns consisting of up to four different "schemes" (each campaign) and directed at up to 5,000 employees (each campaign) to identify areas of improvement in the "people" and "process" parts of the "people, process, and technology" framework and areas of focus for the training and awareness program.

Approach

The phishing engineer will utilize a combination of insider knowledge and the latest trends in phishing to achieve a realistic scenario designed to entice employees into investigating the email and handing over restricted or sensitive information. Findings from this study will provide insight into the

workforce's ability to take a critical eye to suspicious emails as well as deliver reporting about how far into the phishing net they swam. CynergisTek will:

- Send phishing emails to your employees safely and easily.
- Create a unique teachable moment when an employee falls for a simulated attack
- Use that moment to teach the employee how not to fall for future attacks
- Provide four different customizable training options to meet an organization's unique needs
- Gather actionable data to finely target future employee training

You can reduce the chance of employees falling for an attack by 60% with just one mock phishing attack and administrators and security officers collect powerful information to assess where their organizations are most vulnerable.

1.10. Virtual Chief Information Security Officer (vCISO)

Many of our NMCs are finding it increasingly difficult to attract, recruit and retain the highly skilled information security resources that are needed in today's complex, data driven health care setting. With increased reliance on data and information systems, security and privacy are critical components in assuring the reliability, availability and confidentiality of information. CynergisTek has provided reliable information security and privacy services to healthcare entities for more than a decade, focused on building and sustaining data security programs. NMC has engaged CynergisTek to assign a senior information security consultant to serve in a Virtual CISO role, providing dedicated information security expertise and advice in support of its Chief Information Officer, Security Officer and other key staff. The vCISO is not a permanent staff position nor is it designed to relieve the NMC Security Officer of their responsibility for protecting information assets.

The CynergisTek vCISO program is a three year program designed to guide NMCs through the costly and cumbersome process of defining, deploying, and managing an information security program. At the end of the initial period of support the NMC may then elect to insource or renew at the then current rate indefinitely.

Focus areas for the program are intended to help address the following:

- Complex Decisions
  - Often reactionary and tactical to satisfy a specific audit finding without considering the big picture.
  - Made without a clear understanding of who will have responsibility for the end product.
  - Tactical decisions without thorough understanding of the strategic goals
  - Costly, since eventually these solutions fall short of compliance or are not operationally sustainable
- Spur of the moment deployment strategy
  - Implemented to satisfy an audit finding
  - Inexperienced; immature admin and deployment
  - Higher risk by design or, often minimal utilization and eventually become shelf-ware
- Managing costs and business expectations
  - Limited Operations - the day-to-day information security tasks
  - Always a fire drill - compliance tasks that fall off the radar
  - Working harder - Areas of automation and a decision's total cost of ownership

There must be a baseline assessment performed to jumpstart and act as input into this process. As an existing CAPP customer, the most recent annual assessment will serve this purpose. It should be noted that this service is not intended to provide or replace full time information security personnel, so the prerequisite risk assessment serves to inform us of work that should be categorized into small, results-oriented consulting opportunities (big example: construct a secure standard for server builds; small example: install a firewall). To help ensure proper funding, these opportunities will take place during the course of three or more budget cycles. During the first meeting of the second month, the

vCISO will present priorities for projects, and after reaching agreement and approval, develop a Plan of Action and Milestones (POAM) which will be a living document. The service is designed to give the NMC the maximum flexibility in using this resource and approach.

Scope

The goal of the vCISO program is to provide experienced certified security consulting to assist the NMC in establishing, improving or managing an appropriate and effective security program capable of not only meeting compliance requirements, but also managing the demands of the business. To achieve this goal for existing CAPP NMCs CynergisTek assigns a primary consultant to work directly with the NMC's IT management or Security Officer. Because existing CAPP NMCs have on-going advisory services and CynergisTek has previous experience through its assessment activities, the initial on-site orientation period is at the discretion of the NMC in consultation with their assigned vCISO. This is accomplished through an amendment to the CAPP adding a block of hours to be used to support on-site and remote CISO support in addition to those CAPP core services. An on-site orientation is still advised to establish key relationships, conduct appropriate environmental surveys, review security current state maturity, priorities and develop the initial Plan of Action and Milestones (POAM). Following this orientation process both on-site and remote activity will be driven as appropriate by the POAM.

Monthly project status meetings will be held with the NMC sponsor and the CynergisTek Program Management Office to review progress. Each supporting project will be reviewed and evaluated as part of a continual improvement process that will inform the security program control selection and implementation tasks. This review process will identify areas of the security program that need to be adjusted to support the needs of the business. The POAM will be updated prior to and after each Monthly status meeting.

Additionally the CynergisTek consultant assigned will establish periodic meetings with their counterpart and other key stake holders to measure progress of the information security program, maintain good communications and audit progress against established goals. CynergisTek will attend and support meetings as requested by the NMC. These can include governance meetings such as a privacy and security committee meetings, risk management meetings, or meetings with executive leadership, etc.

CynergisTek's consultant will coordinate and provide mentoring and training support to NMC personnel assigned security related responsibilities. They will identify any formal training or certifications NMC personnel should have or achieve in order to perform their duties competently. They will provide periodic security education and awareness sessions and provide periodic reminders on security for the NMC workforce at large. Finally, CynergisTek will serve as the principle advisor to the NMC CIO and other Senior staff members as requested and provide support to matters involving information security decisions.

The initial block of hours to support ongoing vCISO activities is set at 300 per year.

Approach

CynergisTek provides experienced security professionals who have held both strategic and tactical roles in large, complex information security programs as well as in small organizations to assist NMCs in building or supporting their information security and risk management programs. The process begins with an initial planning session and then orientation and review of existing assessments, security policies, security program documentation and operational processes. This review will inform the identification of objectives and priorities for improving the security program. These will be captured in the POAM which will become a living action plan that will be updated monthly to reflect progress, current state and future initiatives.

The vCISO support project is based on a block of hours added to the CAPP to provide dedicated CISO support. The number of hours, is established as a minimum not to exceed with out specific written

authorization of the NMC which can be accomplished through regular mail, email, or TekTrak (NMC portal). vCISO support will run coterminous with its associated CAPP agreement. At the initial planning session the number of hours to allocate to the on-site orientation will be determined, a schedule for monthly meetings established and a list of any short term priorities identified for the vCISO to begin addressing. Once the orientation has been completed the assigned vCISO will coordinate directly with their NMC counterpart and follow the POAM. CynergisTek will track hours spent on assigned tasks and provide an accounting at each monthly review meeting. The hours for any given year expire at the end of that 12 month period. To ensure that all interested parties stay abreast of project status and efforts undertaken, CynergisTek will utilize a roll-up report distributed quarterly for governance, risk management, operational, and project updates that will serve as the vehicle for communicating progress and outstanding requirements.

2. PROJECT MANAGEMENT AND LOGISTICS

2.1. TEKTRAK PROJECT MANAGEMENT PORTAL

CynergisTek uses a secure, proprietary project management portal we call TekTrak. All project stakeholders and participants from both sides of the project will be granted access to the TekTrak project providing participants with 24/7 visibility to all project activities. A detailed project plan will be posted in TekTrak that consists of:

- Milestones
- Task Lists (delineated for each major activity)
- Assigned Responsibility for Milestones/Tasks
- Due Dates to Outline the Overall Timeline

All project communications are documented in TekTrak providing a holistic and realtime view into the project progress.

2.2. PROJECT LAUNCH MEETING

The Project Launch Meeting is designed to facilitate mutual understanding for project scope, approach, roles, responsibilities, objectives, project planning, scheduling, and communication. The meeting provides an opportunity for the joint project team to establish a relationship and coordinate the logistics of the project.

While attendance at this meeting is open to all those involved in the project, it is highly recommended that the following attend:

- Project Executive/Sponsor (A NMC-side sponsor of the project on whose direction/authority this project is being executed)
- Project Liaison/Manager (A NMC-side person tasked with day-to-day management of the project and management of the project scheduling/planning)
- Technical Liaison (A NMC-side person tasked with coordinating technical activities within IT/IS)
- Information Security Officer/Manager
- Network Manager
- Privacy Officer/Manager (if applicable)

Other personnel that are suggested as good candidates to include in the attendee list for the project launch meeting include:

- Compliance Manager
- HR Manager
- IT Manager

2.3. INTERACTIVE WORKSHOP

An interactive workshop is scheduled at the conclusion of the engagement for the benefit our NMCs. It is designed to facilitate a mutual understanding of the contents of the Reports of Findings and associated vulnerability reports, as well as facilitate discussion around the observations and recommendations. It also serves as a driver for the NMC's executive and technical teams to continue improving the organization's security program and provides an actionable plan for next steps.

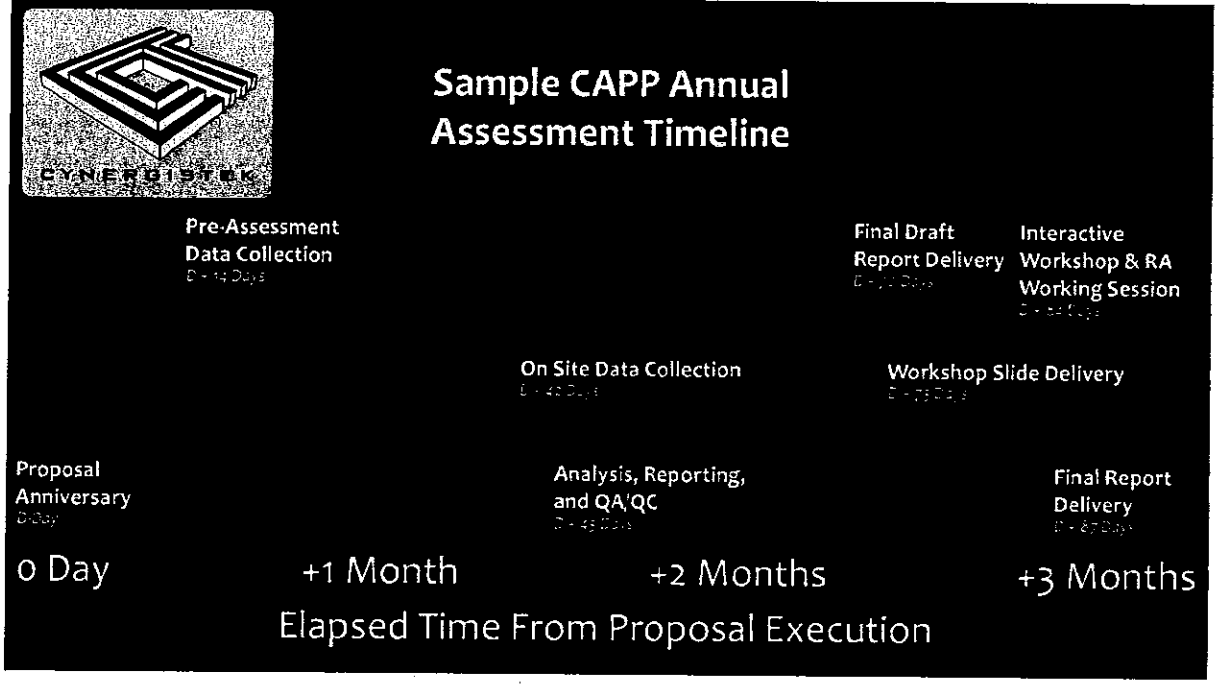
The workshop is typically divided into four (4) sessions that are designed for the appropriate audience and are intended to fit into one day:

- Executive Session - 30-45 Minutes

- Attendee(s): Senior Management from Information Security, Human Resources, Compliance, Physical Security, IT Audit, Privacy, Legal, Finance
- Information Security Program Assessment Session - 1.5 Hours
  - Attendee(s): Management/Staff from Information Security, Human Resources, Compliance, Physical Security, IT Audit, Privacy, Legal, Finance
- Technical Security Assessment - 1.5 Hours
  - Attendee(s): Management/Staff from Network Team, Server Team, Workstation/Laptop/Mobile Device Team, Applications Team, Information Security Team
- Risk Analysis Session - 1.5 Hours
  - Attendee(s): Management/Staff from Information Security, Human Resources, Compliance, Physical Security, IT Audit, Privacy, Legal, Finance

2.4. EXAMPLE PROJECT TIMELINE

The Compliance Assist Partner Program is designed to provide a thorough annual assessment that is augmented by periodic technical testing during the balance of the year. As such the services are spread evenly throughout the year as illustrated in the project overview timeline shown below. The second timeline graphic illustrates further detail around the annual assessment activities depicted on the overview timeline. CynergisTek typically completes the assessment activities across a 10-12 week period starting with Day 0 on each anniversary date of the Proposal (as hereinafter defined).


CYNERGISTEK
Sample CAPP Annual Assessment Timeline
Pre-Assessment Data Collection
Final Draft Report Delivery
Interactive Workshop & RA Working Session
On Site Data Collection
Workshop Slide Delivery
Proposal Anniversary
Analysis, Reporting, and QA/QC
Final Report Delivery
0 Day
+1 Month
+2 Months
+3 Months
Elapsed Time From Proposal Execution

3. DELIVERABLES

Consulting activities and the associated deliverable output outlined in this Proposal are neither intended nor offered as legal advice. CynergisTek's staff, directors, and executives are not practicing attorneys and the relationship between CynergisTek and NMC cannot and must not be construed as an attorney-NMC relationship unless CynergisTek has been engaged specifically through counsel to secure attorney-NMC privilege for the engagement. As such, our consulting and deliverable output are intended for educational and information purposes only. They are neither legal advice nor legal opinions on a specific matter. NMC should neither act nor fail to act on any legal matter based upon either the consulting activities or the deliverable output without first engaging a competent attorney licensed to practice law in the specific jurisdiction in question.

3.1. PROJECT MANAGEMENT AND LOGISTICS

As part of our project management activities and final presentation of results, we include the following in all engagements:

- Project Launch Meeting and Slide Deck (once at the start of the engagement)
- Interactive Findings Workshop and Slide Deck (once per year following each annual assessment)

3.2. RAW VULNERABILITY TESTING REPORTS

We provide raw vulnerability testing reports in dynamic HTML format to serve as a guide to remediation of individual vulnerabilities sorted in two different ways:

- Sort by Host — Shows all hosts individually and the vulnerabilities that were detected on each host as a secondary index. (quarterly for external testing and twice annually for internal testing)
- Sort by Vulnerability — Shows all vulnerabilities individually and the hosts on which they were detected as the secondary index. (quarterly for external testing and twice annually for internal testing)

In addition, we provide an executive summary (usually one page) with graphs, charts, and other general statistics without any of the supporting technical data to share with the executive management team. The executive summary reports will be provided quarterly for external testing and twice annually for internal testing.

3.3. REPORTS OF FINDINGS

Our custom analysis and reporting culminates in the development of our reports of findings. All reports of findings include an executive over and summary, detailed findings and observations, and recommendations for meeting compliance and/or best practice. The following reports will be provided as part of this engagement:

- Technical Security Assessment Report of Findings (once per year following each annual assessment)
  - External Security Assessment
  - Architecture Assessment (includes relevant findings from the Wireless LAN Security Validation)
  - Internal Security Assessment
- Information Security Program Assessment Report of Findings (once per year following each annual assessment) (includes relevant findings from the Meaningful Use EHR Assessment)
- Risk Analysis (once per year following each annual assessment)
  - Risk Analysis Workbook
  - Risk Profile

4. NMC RESPONSIBILITIES

We would like to specifically call out the following items as being key client responsibilities and critical to the success of the engagement:

- Timely and effective communication with particular emphasis on the timely exchange of information and scheduling.
- A commitment to leverage the project management portal, TekTrak, to its fullest extent.
- Assignment of a client-side executive sponsor to endorse and communicate the nature of the project internally.
- Assignment of a client-side Project Liaison to act as a project manager and single point of contact for the project
- Despite both our and our scanning vendor's (Qualys) best efforts to minimize impact to production networks during vulnerability scanning, the fact remains that vulnerability testing does bear the inherent risk of disrupting services. Out of an abundance of caution we request that when submitting the asset lists to be included in vulnerability testing that two very specific asset lists be included
  - Exclusion List - A list of assets that should never be scanned.
  - Critical Asset List - A special list of assets that we 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.
- Coordination with CynergisTek's Operations Coordinator to schedule any/all client-side interviews with stakeholders as early as is feasibly possible after confirmation that on site data collection dates are firm.

5. COMPENSATION AND AUTHORIZATION

CynergisTek will complete all tasks in this Proposal and provide all listed deliverables for a fixed fee of $38,100.00/quarter including travel related expenses. An initial payment of $38,100.00 is due upon completion of the first milestone as identified in Section 2.4.

Invoicing will continue quarterly for a minimum term of three years from execution (Oct-1-2016 to Sept-30-2019).

Further, it is agreed between CynergisTek and NMC that services performed under this Proposal will be performed using reasonable care and skill reflecting the level of knowledge and expertise possessed by those individuals performing the services at time such services are performed. NMC understands and agrees that new technology, configuration changes, software upgrades and routine maintenance, among other items, can create new and unknown security exposures. Moreover, computer "hackers" and other third parties continue to employ increasingly sophisticated techniques and tools, resulting in ever-growing challenges to individual computer system security. It is NMC's sole responsibility to maintain the security of its computer systems.

This Proposal and the prices expressed herein are valid through 30-Oct-16.

NMC	**CynergisTek, Inc.**
_____	_____
Signature	Signature
_____	Dr. Michael G. Mathews, President & COO
Printed Name & Title	Printed Name and Title
_____	01-Sep-16
Date	Date

Exhibit B

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement"), effective October 1, , 20 16 ("Effective Date"), is entered into by and among the County of Monterey, a political subdivision of the State of California, on behalf of Natividad Medical Center ("Covered Entity") and CynergisTek, Inc. ("Business Associate") (each a "Party" and collectively the "Parties").

Business Associate provides certain services for Covered Entity ("Services") that involve the use and disclosure of Protected Health Information that is created or received by Business Associate from or on behalf of Covered Entity ("PHI"). The Parties are committed to complying with the Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subparts A and E as amended from time to time (the "Privacy Rule"), and with the Security Standards, 45 C.F.R. Part 160 and Part 164, Subpart C as amended from time to time (the "Security Rule"), under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health Act and its implementing regulations ("HITECH"). Business Associate acknowledges that, pursuant to HITECH, 45 C.F.R. §§ 164.308 (administrative safeguards), 164.310 (physical safeguards), 164.312 (technical safeguards), 164.316 (policies and procedures and documentation requirements) and 164.502 *et. seq.* apply to Business Associate in the same manner that such sections apply to Covered Entity. The additional requirements of Title XIII of HITECH contained in Public Law 111-005 that relate to privacy and security and that are made applicable with respect to covered entities shall also be applicable to Business Associate. The Parties are also committed to complying with the California Confidentiality of Medical Information Act, Ca. Civil Code §§ 56 *et seq.* ("CMIA"), where applicable. Business Associate acknowledges that the CMIA prohibits Business Associate from further disclosing the PHI it receives from Covered Entity where such disclosure would be violative of the CMIA. The Parties are also committed to complying with applicable requirements of the Red Flag Rules issued pursuant to the Fair and Accurate Credit Transactions Act of 2003 ("Red Flag Rules"). This Agreement sets forth the terms and conditions pursuant to which PHI, and, when applicable, Electronic Protected Health Information ("EPHI"), shall be handled. The Parties further acknowledge that state statutes or other laws or precedents may impose data breach notification or information security obligations, and it is their further intention that each shall comply with such laws as well as HITECH and HIPAA in the collection, handling, storage, and disclosure of personal data of patients or other personal identifying information exchanged or stored in connection with their relationship.

The Parties agree as follows:

1. DEFINITIONS

All capitalized terms used in this Agreement but not otherwise defined shall have the meaning set forth in the Privacy Rule, Security Rule and HITECH.

2. PERMITTED USES AND DISCLOSURES OF PHI

2.1 Unless otherwise limited herein, Business Associate may:

(a) use or disclose PHI to perform functions, activities or Services for, or on behalf of, Covered Entity as requested by Covered Entity from time to time, provided that such use or disclosure would not violate the Privacy or Security Rules or the standards for Business Associate Agreements set forth in 45 C.F.R. § 164.504(e), exceed the minimum necessary to accomplish the intended purpose of such use or disclosure, violate the additional requirements of HITECH contained in Public Law 111-005 that relate to privacy and security, or violate the CMIA;

(b) disclose PHI for the purposes authorized by this Agreement only: (i) to its employees, subcontractors and agents; (ii) as directed by this Agreement; or (iii) as otherwise permitted by the terms of this Agreement;

(c) use PHI in its possession to provide Data Aggregation Services to Covered Entity as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B);

(d) use PHI in its possession for proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate as permitted by 45 C.F.R. § 164.504(e)(4)(i);

(e) disclose the PHI in its possession to third parties for the proper management and administration of Business Associate to the extent and in the manner permitted under 45 C.F.R. § 164.504(e)(4)(ii); provided that disclosures are Required by Law , or Business Associate obtains reasonable assurances from the persons to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached;

(f) use PHI to report violations of law to appropriate Federal and state authorities, consistent with 45 C.F.R. § 164.502(j)(1);

(g) de-identify any PHI obtained by Business Associate under this Agreement for further use or disclosure only to the extent such de-identification is pursuant to this Agreement, and use such de-identified data in accordance with 45 C.F.R. § 164.502(d)(1).

3. RESPONSIBILITIES OF THE PARTIES WITH RESPECT TO PHI

3.1 Responsibilities of Business Associate. With regard to its use and/or disclosure of PHI, Business Associate shall:

(a) use and/or disclose the PHI only as permitted or required by this Agreement or as otherwise Required by Law;

(b) report to the privacy officer of Covered Entity, in writing, (i) any use and/or disclosure of the PHI that is not permitted or required by this Agreement of which Business Associate becomes aware, and (ii) any Breach of unsecured PHI as specified by HITECH, within two (2) days of Business Associate's determination of the occurrence of such unauthorized use and/or disclosure. In such event, the Business Associate shall, in consultation with the Covered Entity, mitigate, to the extent practicable, any harmful effect that is known to the Business Associate of such improper use or disclosure. The notification of any Breach of unsecured PHI shall include, to the extent possible, the identification of each individual whose unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, used or disclosed during the Breach.

(c) use commercially reasonable safeguards to maintain the security of the PHI and to prevent use and/or disclosure of such PHI other than as provided herein;

(d) obtain and maintain an agreement with all of its subcontractors and agents that receive, use, or have access to, PHI pursuant to which agreement such subcontractors and agents

agree to adhere to the same restrictions and conditions on the use and/or disclosure of PHI that apply to Business Associate pursuant to this Agreement;

(e) make available all internal practices, records, books, agreements, policies and procedures and PHI relating to the use and/or disclosure of PHI to the Secretary for purposes of determining Covered Entity or Business Associate's compliance with the Privacy Rule;

(f) document disclosures of PHI and information related to such disclosure and, within ten (10) days of receiving a written request from Covered Entity, provide to Covered Entity such information as is requested by Covered Entity to permit Covered Entity to respond to a request by an individual for an accounting of the disclosures of the individual's PHI in accordance with 45 C.F.R. § 164.528, as well as provide an accounting of disclosures, as required by HITECH, directly to an individual provided that the individual has made a request directly to Business Associate for such an accounting. At a minimum, the Business Associate shall provide the Covered Entity with the following information: (i) the date of the disclosure, (ii) the name of the entity or person who received the PHI, and if known, the address of such entity or person; (iii) a brief description of the PHI disclosed; and (iv) a brief statement of the purpose of such disclosure which includes an explanation of the basis for such disclosure. In the event the request for an accounting is delivered directly to the Business Associate, the Business Associate shall, within two (2) days, forward such request to the Covered Entity. The Business Associate shall implement an appropriate recordkeeping process to enable it to comply with the requirements of this Section;

(g) subject to Section 4.4 below, return to Covered Entity within twenty-one (21) days of the termination of this Agreement, the PHI in its possession and retain no copies, including backup copies;

(h) disclose to its subcontractors, agents or other third parties, and request from Covered Entity, only the minimum PHI necessary to perform or fulfill a specific function required or permitted hereunder;

(i) if all or any portion of the PHI is maintained in a Designated Record Set:

(i) upon ten (10) days' prior written request from Covered Entity, provide access to the PHI in a Designated Record Set to Covered Entity or, as directed by Covered Entity, the individual to whom such PHI relates or his or her authorized representative to meet a request by such individual under 45 C.F.R. § 164.524; and

(ii) upon ten (10) days' prior written request from Covered Entity, make any amendment(s) to the PHI that Covered Entity directs pursuant to 45 C.F.R. § 164.526;

(j) maintain policies and procedures to detect and prevent identity theft in connection with the provision of the Services, to the extent required to comply with the Red Flag Rules;

(k) notify the Covered Entity within five (5) days of the Business Associate's receipt of any request or subpoena for PHI. To the extent that the Covered Entity decides to assume responsibility for challenging the validity of such request, the Business Associate shall cooperate fully with the Covered Entity in such challenge;

(l) maintain a formal security program materially in accordance with all applicable data security and privacy laws and industry standards designed to ensure the security and integrity of the Covered Entity's data and protect against threats or hazards to such security

The Business Associate acknowledges that, as between the Business Associate and the Covered Entity, all PHI shall be and remain the sole property of the Covered Entity.

3.2 Additional Responsibilities of Business Associate with Respect to EPHI. In the event that Business Associate has access to EPHI, in addition to the other requirements set forth in this Agreement relating to PHI, Business Associate shall:

(a) implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of EPHI that Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity as required by 45 C.F.R. Part 164, Subpart C;

(b) ensure that any subcontractor or agent to whom Business Associate provides any EPHI agrees in writing to implement reasonable and appropriate safeguards to protect such EPHI; and

(c) report to the privacy officer of Covered Entity, in writing, any Security Incident involving EPHI of which Business Associate becomes aware within two (2) days of Business Associate's discovery of such Security Incident. For purposes of this Section, a Security Incident shall mean (consistent with the definition set forth at 45 C.F.R. § 164.304), the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system. In such event, the Business Associate shall, in consultation with the Covered Entity, mitigate, to the extent practicable, any harmful effect that is known to the Business Associate of such improper use or disclosure.

3.3 Responsibilities of Covered Entity. Covered Entity shall, with respect to Business Associate:

(a) provide Business Associate a copy of Covered Entity's notice of privacy practices ("Notice") currently in use;

(b) notify Business Associate of any limitations in the Notice pursuant to 45 C.F.R. § 164.520, to the extent that such limitations may affect Business Associate's use or disclosure of PHI;

(c) notify Business Associate of any changes to the Notice that Covered Entity provides to individuals pursuant to 45 C.F.R. § 164.520, to the extent that such changes may affect Business Associate's use or disclosure of PHI;

(d) notify Business Associate of any changes in, or withdrawal of, the consent or authorization of an individual regarding the use or disclosure of PHI provided to Covered Entity pursuant to 45 C.F.R. § 164.506 or § 164.508, to the extent that such changes may affect Business Associate's use or disclosure of PHI; and

(e) notify Business Associate, in writing and in a timely manner, of any restrictions on use and/or disclosure of PHI as provided for in 45 C.F.R. § 164.522 agreed to by Covered Entity, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

4. TERMS AND TERMINATION

4.1 Term. This Agreement shall become effective on the Effective Date and shall continue in effect unless terminated as provided in this Article 4. Certain provisions and requirements of this Agreement shall survive its expiration or other termination as set forth in Section 5.1 herein.

4.2 Termination. Either Covered Entity or Business Associate may terminate this Agreement and any related agreements if the terminating Party determines in good faith that the terminated Party has breached a material term of this Agreement; provided, however, that no Party may terminate this Agreement if the breaching Party cures such breach to the reasonable satisfaction of the terminating Party within thirty (30) days after the breaching Party's receipt of written notice of such breach.

4.3 Automatic Termination. This Agreement shall automatically terminate without any further action of the Parties upon the termination or expiration of Business Associate's provision of Services to Covered Entity.

4.4 Effect of Termination. Upon termination or expiration of this Agreement for any reason, Business Associate shall return all PHI pursuant to 45 C.F.R. § 164.504(e)(2)(ii)(I) if, and to the extent that, it is feasible to do so. Prior to doing so, Business Associate shall recover any PHI in the possession of its subcontractors or agents. To the extent it is not feasible for Business Associate to return or destroy any portion of the PHI, Business Associate shall provide Covered Entity a statement that Business Associate has determined that it is infeasible to return or destroy all or some portion of the PHI in its possession or in possession of its subcontractors or agents. Business Associate shall extend any and all protections, limitations and restrictions contained in this Agreement to any PHI retained after the termination of this Agreement until such time as the PHI is returned to Covered Entity or destroyed.

5. MISCELLANEOUS

5.1 Survival. The respective rights and obligations of Business Associate and Covered Entity under the provisions of Sections 4.4, 5.1, 5.6, and 5.7, and Section 2.1 (solely with respect to PHI that Business Associate retains in accordance with Section 4.4 because it is not feasible to return or destroy such PHI), shall survive termination of this Agreement until such time as the PHI is returned to Covered Entity or destroyed. In addition, Section 3.1(i) shall survive termination of this Agreement, provided that Covered Entity determines that the PHI being retained pursuant to Section 4.4 constitutes a Designated Record Set.

5.2 Amendments; Waiver. This Agreement may not be modified or amended, except in a writing duly signed by authorized representatives of the Parties. To the extent that any relevant provision of the HIPAA, HITECH or Red Flag Rules is materially amended in a manner that changes the obligations of Business Associates or Covered Entities, the Parties agree to negotiate in good faith appropriate amendment(s) to this Agreement to give effect to the revised obligations. Further, no provision of this Agreement shall be waived, except in a writing duly signed by authorized representatives of the Parties. A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events.

5.3 No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the Parties and the respective successors or assigns of the Parties, any rights, remedies, obligations, or liabilities whatsoever.

5.4 Notices. Any notices to be given hereunder to a Party shall be made via U.S. Mail or express courier to such Party's address given below, and/or via facsimile to the facsimile telephone numbers listed below.

If to Business Associate, to:
CynergisTek Inc.
11410 Jollyville Road, Suite 2201
Austin, TX 78759
Attn: Adam Hawkins, Vice President, Sales & Marketing
Phone: 512 402-8550
Fax: 512 857-0700

If to Covered Entity, to:
Natividad Medical Center
1441 Constitution Blvd.
Salinas, CA 93906
Attn: Contracts Division
Phone: 831-755-4111
Fax: 831-757-2592

Each Party named above may change its address and that of its representative for notice by the giving of notice thereof in the manner hereinabove provided. Such notice is effective upon receipt of notice, but receipt is deemed to occur on next business day if notice is sent by FedEx or other overnight delivery service.

5.5 Counterparts; Facsimiles. This Agreement may be executed in any number of counterparts, each of which shall be deemed an original. Facsimile copies hereof shall be deemed to be originals.

5.6 Choice of Law; Interpretation. This Agreement shall be governed by the laws of the State of California; as provided, however, that any ambiguities in this Agreement shall be resolved in a manner that allows Business Associate to comply with the Privacy Rule, and, if applicable, the Security Rule and the CMIA.

5.7 Indemnification. Contractor shall indemnify, defend, and hold harmless the County of Monterey (hereinafter County), its officers, agents, and employees from any claim, liability, loss, injury, cost, expense, penalty or damage, including the County's reasonable cost of providing notification of and of mitigating any acquisition, access, use or disclosure of PHI in a manner not permitted by this BAA, arising out of, or in connection with, performance of this BAA by Contractor and/or its agents, members, employees, or sub-contractors, excepting only loss, injury, cost, expense, penalty or damage caused by the negligence or willful misconduct of personnel employed by the County. It is the intent of the parties to this BAA to provide the broadest possible indemnification for the County. Contractor shall reimburse the County for all costs, attorneys' fees, expenses, and liabilities incurred by the County with respect to any investigation, enforcement proceeding or litigation in which Contractor is obligated to indemnify, defend, and hold harmless the County under this BAA. This provision is in addition to and independent of any indemnification provision in any related or other agreement between the Covered Entity and the Business Associate.

IN WITNESS WHEREOF, each of the undersigned has caused this Agreement to be duly executed in its name and on its behalf as of the Effective Date.

[BUSINESS ASSOCIATE]	*COUNTY OF MONTEREY, ON BEHALF OF NATIVIDAD MEDICAL CENTER*
By: _____	By: _____
Print Name: Dr. Michael G. Mathews	Print Name: _____
Print Title: President & COO	Print Title: _____
Date: 01-Sep-16	Date: _____

ADDENDUM #1

TO AGREEMENT BY AND BETWEEN CYNERGISTEK, INC. AND THE COUNTY OF MONTEREY ON BEHALF OF NATIVIDAD MEDICAL CENTER FOR INFORMATION SECURITY SERVICES

This Addendum #1 amends, modifies, and supplements the County of Monterey Agreement for Services (hereinafter "Agreement") by and between CONTRACTOR, INC. (hereinafter "CONTRACTOR") and the County of Monterey, on behalf of Natividad Medical Center (hereinafter "NMC"). This Addendum #1 has the full force and effect as if set forth within the terms and conditions of the Agreement. To the extent that any of the terms or conditions contained in this Addendum #1 may contradict or conflict with any of the terms and conditions of the Agreement, it is expressly understood and agreed that the terms and conditions of this Addendum #1 shall take precedence and supersede the attached Agreement.

NOW, THEREFORE, NMC and CONTRACTOR agree that the Agreement terms and conditions shall be amended, modified, and supplemented as follows:

I. Agreement paragraph 3.2 under "TERM OF AGREEMENT", shall be amended to:

3.2 Notwithstanding anything contained in this Agreement to the contrary, if insufficient funds are appropriated, or funds are otherwise unavailable in the budget for NMC for any reason whatsoever in any fiscal year, for payments due under this Agreement, NMC will immediately notify CONTRACTOR of such occurrence, and this AGREEMENT shall terminate after the last day during the fiscal year for which appropriations shall have been budgeted for NMC or are otherwise available for payments.

II. Agreement paragraph 8.1 under "INDEMNIFICATION", shall be amended to:

8.1 CONTRACTOR shall indemnify, defend, and hold harmless the County (including NMC), its officers, agents and employees from any claim, liability, loss, injury or damage directly rising out of, or in direct connection with, performance of this Agreement by CONTRACTOR and/or its agents, members, employees or sub-contractors, excepting only loss, injury or damage caused by the negligence or willful misconduct of personnel employed by NMC. It is the intent of the Parties to this Agreement to provide the broadest possible indemnification for NMC. CONTRACTOR shall reimburse NMC for all costs, attorneys' fees, expenses and liabilities incurred by NMC with respect to any litigation in which CONTRACTOR is obligated to indemnify, defend and hold harmless NMC under this Agreement.

NMC shall indemnify, defend, and hold harmless CONTRACTOR, its officers, agents and employees from any claim, liability, loss, injury or damage arising out of, or in connection with, performance of this Agreement by the County (including NMC) and/or its agents, members, employees or sub-contractors, excepting only loss, injury or damage caused by the negligence or willful misconduct of personnel employed by

CONTRACTOR. It is the intent of the Parties to this Agreement to provide the broadest possible coverage for CONTRACTOR. NMC shall reimburse CONTRACTOR for all costs, attorneys' fees, expenses and liabilities incurred by CONTRACTOR with respect to any litigation in which NMC is obligated to indemnify, defend and hold harmless CONTRACTOR under this Agreement.

III. An additional paragraph 15.17, "LIMITED WARRANTY" shall be added as follows:

15.17 LIMITED WARRANTY. CONTRACTOR warrants to NMC that the Services will be of the kind and quality expressly designated in the Statement of Work and will be performed by qualified personnel. Any special requirements for format standards or methods to be followed shall be included in the Statement(s) of Work and executed by both NMC and CONTRACTOR. In the event of a breach of the foregoing warranty, CONTRACTOR sole obligation shall be to (a) correct any material error so as to bring the Deliverables into compliance therewith or (b) reimburse NMC up to but not in excess of the aggregate insurance requirements' dollar limits stated within the Agreement paragraph 9.3. Any claim for breach of the foregoing warranty must be made by written notice to CONTRACTOR within ninety (90) days of CONTRACTOR's delivery of any or all Deliverables. This is a contract for services and is not governed by the Uniform Commercial Code. EXCEPT AS PROVIDED IN THIS SECTION, CONTRACTOR MAKES NO OTHER WARRANTIES OR REPRESENTATIONS WHETHER EXPRESS OR IMPLIED, ARISING BY LAW, CUSTOM, ORAL OR WRITTEN STATEMENTS OF CONTRACTOR, ITS AGENTS, OFFICERS, SHAREHOLDERS, SUBCONTRACTORS OR OTHERWISE, AND SPECIFICALLY DISCLAIMS THE WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE ARE HEREBY SUPERSEDED, EXCLUDED AND DISCLAIMED.

NMC understands and agrees that CONTRACTOR shall have no responsibility for or be liable to any extent for any hardware, software or other items or property manufactured or prepared by anyone other than CONTRACTOR.

NMC represents and warrants to CONTRACTOR that, with respect to any software it asks CONTRACTOR to modify, NMC has the authority to engage a third party to modify such software. For all such requested modifications, NMC shall provide applicable third party documentation as may be requested by CONTRACTOR. NMC also represents and warrants that for all third party documentation which it provides, that it has the authority to provide such documentation to CONTRACTOR for CONTRACTOR's use in such requested modifications. NMC shall indemnify, hold harmless and defend CONTRACTOR, its officers and directors, shareholders, employees, agents and subcontractors, at NMC's sole cost and expense, from any and all claims against CONTRACTOR alleging copyright or other infringement for software modifications made by CONTRACTOR. If a suit for copyright infringement is filed against CONTRACTOR based upon the aforementioned modifications, NMC shall have the right to select the defense counsel who NMC is

to provide, subject to CONTRACTOR's right to approve such defense counsel selected by NMC.

Notwithstanding any provision of the Contract to the contrary, the Parties agree that in no event shall CONTRACTOR's aggregate liability to NMC under this Contract, regardless of the character or type of damages sought or the theory of such liability, exceed the aggregate insurance requirements' dollar limits stated within the attached Agreement paragraph 9.3.

No actions or disputes, regardless of form, arising out of any Services, may be brought by either Party more than one (1) year after the termination of this Agreement.