Natividad MEDICAL CENTER

County of Monterey Agreement for Services
(Not to Exceed $100,000)

This Agreement (hereinafter "Agreement") is made by and between the County of Monterey, a political subdivision of the State of California, on behalf of Natividad Medical Center, an acute care hospital (hereinafter, "NMC"), and tw-Security, LLC hereinafter "CONTRACTOR (collectively, the County and CONTRACTOR are referred to as the "Parties.").

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

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 HIPAA compliance programs (Security, Privacy, and Breach Notification).

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 $68,750.

TERM OF AGREEMENT; the term of this Agreement is from January 1, 2021 through December 31, 2021 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.

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

SCOPE OF SERVICES AND 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: County of Monterey Travel and Business Expense Reimbursement Policy
Business Associate Agreement

1. PERFORMANCE STANDARDS:

1.1. 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.

1.2. 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.

1.3. 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.

2. PAYMENT CONDITIONS:

2.1. Prices shall remain firm for the initial term of the Agreement and, thereafter, may be adjusted annually as provided herein. NMC (Monterey County) does not guarantee any minimum or maximum amount of dollars to be spent under this Agreement.

2.2. Negotiations for rate changes shall be commenced, by CONTRACTOR, a minimum of ninety days (90) 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.

2.3. CONTRACTOR shall submit to the Contract Administrator an invoice on a form acceptable to NMC. If not otherwise specified, the CONTRACTOR may 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 Administrator or his or her designee 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.

2.4. CONTRACTOR shall not receive reimbursement for travel expenses unless set forth in this Agreement.

3. TERMINATION:

3.1. 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.

3.2. 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.

4. INDEMNIFICATION:

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

5. INSURANCE:

5.1. 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 the Contractor.

5.2. 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.

5.3. 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:

5.4. 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.

(Note: any proposed modifications to these general liability insurance requirements shall be attached as an Exhibit hereto, and the section(s) above that are proposed as not applicable shall be lined out in blue ink. All proposed modifications are subject to County approval.)

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

5.5. 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 $500,000 per occurrence.

(Note: any proposed modifications to these general liability insurance requirements shall be attached as an Exhibit hereto, and the section(s) above that are proposed as not applicable shall be lined out in blue ink. All proposed modifications are subject to County approval.)

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

tw-Security, LLC for HIPAA compliance programs (Security, Privacy, and Breach Notification)

5.6. Workers' Compensation Insurance, If CONTRACTOR employs other 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.

(Note: any proposed modifications to these general liability insurance requirements shall be attached as an Exhibit hereto, and the section(s) above that are proposed as not applicable shall be lined out in blue ink. All proposed modifications are subject to County approval.)

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

5.7. 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.

(Note: any proposed modifications to these general liability insurance requirements shall be attached as an Exhibit hereto, and the section(s) above that are proposed as not applicable shall be lined out in blue ink. All proposed modifications are subject to County approval.)

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

6. Other Insurance Requirements:

6.1. 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.

6.2. 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.

6.3. **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.**

6.4. 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 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.

6.5. 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.

7. RECORDS AND CONFIDENTIALITY:

7.1. 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.

7.2. 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.

7.3. 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.

7.4. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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 Natividad Medical Center 1441Constitution Blvd Salinas, CA. 93906 FAX: 831-757-2592	Name: tw-Security, LLC Attn: Thomas Walsh (Tom) Address: 6108 W 121st Street City, State, Zip: Overland Park, KS 66209 FAX: _____ Email: tom.walsh@tw-Security.com

MISCELLANEOUS PROVISIONS:

13.1 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.

13.2 Amendment. This Agreement may be amended or modified only by an instrument in writing signed by NMC and the Contractor.

13.3 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.

13.4 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.

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

13.6 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.

13.7 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.

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

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

13.10 Time is of the Essence. Time is of the essence in each and all of the provisions of this Agreement.

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

13.12 Non-exclusive Agreement. This Agreement is non-exclusive and both NMC and CONTRACTOR expressly reserve the right to contract with other entities for the same or similar services.

13.13 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.

13.14 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.

13.15 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.

13.16 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.

13.17 Please see Exhibit A tw-Security Master Agreement.

Signature Page to follow

NATIVIDAD MEDICAL CENTER

By: _____
Gary R. Gray, DO, CEO

Date: _____

APPROVED AS TO LEGAL PROVISIONS

By: _____
Monterey County Deputy County Counsel

Date: 12/08/2020

APPROVED AS TO FISCAL PROVISIONS

By: gary k gibonsy
Monterey County Deputy Auditor/Controller

Date: 12-8-2020

CONTRACTOR

tw-Security, LLC
Contractor's Business Name*** (see instructions)

Thomas R. Walsh
Signature of Chair, President, or Vice-President

Thomas R. Walsh (Tom), Founder, Managing Partner
Name and Title

Date: October 2, 2020

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

Fran Hunter, Partner, Business Development
Name and Title

Date: October 2, 2020

***__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 an individual capacity, the individual shall set forth the name of the business, if any and shall personally sign the Agreement (one signature required).

Security
Healthcare Security & Privacy

6108 W. 121st Street, Overland Park, KS 66209
913-396-8321 | CustomerCare@tw-Security.com
https://tw-Security.com

Exhibit A – Scope of Services/Payment Provisions

Prepared for

NMC Medical Center

Statement of Work to Provide

HIPAA and Cybersecurity Programs Evaluation Services

December 1, 2020

Version 3

STATEMENT OF CONFIDENTIALITY

The information in this Statement of Work (SOW) is confidential and proprietary. It has been made available to you solely for your consideration. The details of this SOW will not be disclosed or disseminated without the express written permission of tw-Security.

Contact Information

Organization	NMC Medical Center (NMC)
Address	1441 Constitution Blvd. Salinas, CA 93906
Contact	Ari Entin
Title	Chief Information Officer
Phone	(831) 783-2564
Email	EntinA@NMC.com
URL	www.natividad.com

Table of Contents

Copyright © 2020 tw-Security. ALL RIGHTS RESERVED. Confidential materials. Duplication or disclosure is prohibited without permission.

Introduction and Our Understanding

Thank you for requesting a Statement of Work (SOW) from tw-Security to evaluate Natividad Medical Center's (NMC) ability to demonstrate compliance with the HIPAA Security Rule, Privacy Rule, and Breach Notification requirements, and provide professional services as needed. This SOW describes how tw-Security will provide the requested services. If our understanding does not match your expectations, we would be pleased to work with you in reaching a mutually acceptable agreement on the service offerings.

tw-Security Introduction/Overview

Since 2003, tw-Security has been a recognized leader and trusted advisor in cybersecurity, privacy, and compliance. Our company is dedicated solely to helping healthcare organizations *(covered entities and business associates)* protect their information resources. Using branded methodologies and tools, tw-Security's certified consultants have a proven track record of reliably delivering high-value services.

Multiple healthcare customers have relied on tw-Security's risk analysis, HIPAA programs evaluation, and our tailored Virtual Security/Privacy Officer (VSPO) solution provided through hands-on support and ongoing advisory services for several years, some for almost a decade.

All of tw-Security's customers that have undergone an audit by the Office for Civil Rights (OCR) or Figliozzi and Company *(contractor to The Centers for Medicare & Medicaid Services (CMS))* have passed the core measure for risk analysis.

Our services are grounded in the guiding principles that data privacy is achieved through security. Information security is the cornerstone to maintaining the public trust, is primarily a business issue – not just a technology issue, should be risk-based and cost-effective, and aligned with your priorities, industry-prudent practices, and government requirements.

The combination of our experience in cybersecurity, data privacy, healthcare, and HIPAA make us an ideal partner for NMC to provide the requested services. We have the skills to connect with the board of directors, executives, physicians, PhDs, to technical staff. Leveraging lessons learned, we assist our customers to guide and develop, monitor and maintain, and improve their HIPAA and cybersecurity/privacy programs.

What differentiates us from other consulting firms?

- **Leadership**. A nationally recognized leader in providing healthcare cybersecurity, privacy, and compliance.
- **Stability**. A privately held, partner-owned company that has been in business since 2003.
- **Vendor neutral**. We are not a reseller of products or services.
- **We are results driven**. We follow an 'outcomes' driven methodology for defining, measuring, and reporting project progress that drives on-time, on-budget results.
- **We value your time**. We minimize the time investment required of our customers by keeping the questions linked to threats and focusing on the critical few rather than the trivial many.

Please see **Appendix A: Why tw-Security** and for quotes, articles, publications, podcasts, etc., please visit **www.tw-security.com, Trusted Advisor, In the News**.

Our customers evaluation of our services can be accessed at this hyperlink: KLAS Research

(Copyright ©2020 KLAS Research. All rights reserved.)

Copyright © 2020 tw-Security. ALL RIGHTS RESERVED. Confidential materials. Duplication or disclosure is prohibited without permission.

Services Description

HIPAA Security Rule, Privacy Rule, and Breach Notification Requirements Programs Evaluation

Under the Health Information Technology for Economic and Clinical Health Act (HITECH Act), the Centers for Medicare and Medicaid (CMS) and Office for Civil Rights (OCR), mandated periodic audits of covered entities and business associates to assess their compliance with HIPAA. Therefore, an evaluation is an effective way to understand your compliance posture with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Privacy and Security Rules, and the Breach Notification requirements under the HITECH Act.

The scope of this evaluation is to evaluate compliance with the HIPAA Security and Privacy Rules, and Breach Notification requirements. Our evaluation is intended to present a high-level summary of NMC's HIPAA programs and their key attributes.

Our HIPAA compliance evaluation process is based upon the audit test procedures in the OCR's *HIPAA Audit Program Protocol,* the same audit test procedures used by the Office for Civil Rights (OCR) – the agency responsible for HIPAA enforcement. *Proof of compliance is primarily evidence-based.*

The HIPAA security rule is comprehensive, flexible, scalable, and technology neutral; however, emerging technologies and privacy regulations require diligence to know if you are complying with the intent of the Rules.

We will get an understanding of NMC's current environment and pertinent organizational practices. We will review documentation *(evidence)* – policies, procedures, plans, etc. regarding your current safeguards controls.

Based upon our experience from examining the Resolution Agreements and Corrective Action Plans posted on the Department of Health and Human Services (HHS) website, we know which criteria and circumstances resulted in the OCR assessing a fine on a healthcare provider or business associate. Therefore, this HIPAA programs evaluation is to focus on the critical few versus the trivial many to determine if reasonable care is being taken to secure your protected health information (PHI) and meet the HIPAA rules.

tw-Security's approach to the requested services are based on our experience with:

- The HIPAA Privacy and Security Rules and the Breach Notification requirements
- Criteria included in the *HIPAA Audit Program Protocol* used by HHS Office for Civil Rights (OCR) auditors and investigators as audit test procedures for assessing compliance
    - The OCR's *HIPAA Audit Program Protocol* analyzes processes, controls, and policies of selected covered entities and business associates pursuant to the HITECH Act audit mandate
- Firsthand experience in dealing with OCR investigators and contract auditors for CMS

Copyright © 2020 tw-Security. ALL RIGHTS RESERVED. Confidential materials. Duplication or disclosure is prohibited without permission.

Cybersecurity Maturity Program Evaluation

Using our methods and tools we will evaluate NMC's cybersecurity program, its key attributes and maturity. During the evaluation we will be mindful of other pertinent regulations / standards and identify gaps where apparent. Respective to COVID 19 and to manage costs, services will be provided remotely.

We will incorporate the HHS Office for Civil Rights' (OCR) expected practices, methods, procedures, and processes by using Health Industry Cybersecurity Practices (HICP), created as part of the Cybersecurity Act of 2015, Section 405(d) "Aligning Health Care Industry Security Approaches" as guidance for best/prevailing practices. HICP recognized the *uniqueness of healthcare organizations*, complexity of cybersecurity threats, and that there is no simple method to combat them all. We appreciate HICP's guidance as it is consistent with our historical approach – to focus on the critical few.

Using tw-Security's methods and tools, we will base our cybersecurity program evaluation on criteria defined in Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) technical volume for medium healthcare organizations. HICP, the primary publication of the Cybersecurity Act of 2015, Section 405(d) is aligned with existing information and guidance (e.g. National Institute of Standards and Technology (NIST) Cyber Security Framework and the Center for Internet Security's Top 20 Cyber Security Controls.)

HICP, a joint Health and Human Services (HHS) and industry led initiative aims to increase awareness and foster consistency with cybersecurity practices recognizing the criticality of uninterrupted care delivery and patient safety to serve as a resource for cost-effectively reducing cybersecurity risks for health care organizations. HHS continues to institutionalize cybersecurity as a key priority and is actively advocating the culture shift to treat cybersecurity as an enterprise issue.

HICP's collaborative process defines an appropriate common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, processes and suggested metrics for measuring practice effectiveness for "like" organizations. The following table identifies the cybersecurity program evaluation criteria of the key threats and practices.

Cybersecurity Program Evaluation Criteria	
Key Threats	Practices *(Tailored for a large organization.)*
1. Email phishing attacks 2. Ransomware attacks (or other malware) 3. Loss or theft of equipment or data 4. Insider, accidental or intentional data loss 5. Attacks against connected medical devices that may affect patient safety Beyond the five threats addressed in HICP, we will also address: - Hacking - Vendor vetting/supply chain security	1. Email protection systems 2. Endpoint protection systems 3. Access management 4. Data protection and loss prevention 5. Asset management 6. Network management 7. Vulnerability management 8. Incident response 9. Medical device security 10. Cybersecurity policies

Maturity expectations and targets - Keeping with NMC's current framework, we will measure maturity based on the Capability Maturity Model (CMM). Definitions for each maturity level could be slightly modified to meet NMC's needs. The maturity of controls is one measure we use to inform our recommendations.

Copyright © 2020 tw-Security. ALL RIGHTS RESERVED. Confidential materials. Duplication or disclosure is prohibited without permission.

Prioritized Recommendations - We identify the maturity gap between current and desired state. The recommendations for improvement are presented with an associated level of effort to focus measurable improvements in NMC's security program maturity and capability posture to minimize risk. Also, we profile organizational and operational practices to focus on people and processes to address risks and areas of noncompliance.

Worth noting - While organizations try their best to prevent a cyberattack – no organization is perfect or operates risk free. Adversarial forces are constantly evolving to avoid detection and to improve their chances of a successful attack. This is why tw-Security also closely examines the organization's readiness to respond *(incident response capability)* and to quickly recover *(business continuity and disaster recovery)* from a cyber incident or attack. *Most importantly, at the end of the day it's all about taking care of patients and the business of healthcare.*

HIPAA and Cybersecurity Programs Evaluation Engagement Approach

The HIPAA and cybersecurity programs evaluation engagement steps, work products, and deliverables are outlined in the table below.

HIPAA Compliance and Cybersecurity Programs Evaluation Approach	
Engagement Steps	Deliverables or Work Products
1. Initiate engagement	⎩ Engagement Plan ⎩ Telephone Interview Schedule *(Listing interview topic, objective, and suggested attendee by job title.)* ⎩ Document request list *(Existing documentation and relevant policies, procedures, standards, plans, and forms to support compliance.)* *(Initiation includes planning, preparation, kickoff, and coordination.)*
2. Gather data	⎩ Feedback and recommendations on reviewed documentation *(We will review documentation and conduct interviews to gain an understanding and validate alignment of the current environment of select safeguards, controls, and organizational / operational practices focused on risk, HIPAA compliance, and, urgent threats and practices to mitigate those threats. Review screenshots and documentation that support the validation of select controls.)*
3. Establish maturity expectations and targets	⎩ Target Profile *(Determine realistic maturity targets based upon the NIST Cybersecurity Framework and Capability Maturity Model (CMM))*
4. Analyze data	*(Identify gaps between the regulations and existing documentation, practices, and perceptions.)*

Copyright © 2020 tw-Security. ALL RIGHTS RESERVED. Confidential materials. Duplication or disclosure is prohibited without permission.

HIPAA Compliance and Cybersecurity Programs Evaluation Approach	
Engagement Steps	Deliverables or Work Products
5. Create reports [Drafts and Finals]	⟩ HIPAA Security Rule – Report of Findings and Recommendations ⟩ HIPAA Privacy Rule and Beach Notification – Report of Findings and Recommendations *(Findings and recommendations highlighting strengths, weaknesses, and citing any significant compliance gaps with HIPAA.)* ⟩ HICP Cybersecurity Report) *(The Report includes a summary of findings, metrics, and prioritized improvement initiatives. The Draft report is amended based on feedback. The Final report will serve as a roadmap to decrease risk (key threats) and increase NMC's Cyber Security Program maturity.)*
6. Create action plan	⟩ Prioritized Action Plan
7. Provide knowledge transfer	⟩ Executive presentation *(Create and deliver a presentation of NMC's HIPAA compliance status and cybersecurity program findings, recommendations, engagement methodology and metrics.)* ⟩ Additional handouts *(samples)* to support knowledge transfer
8. Conclude engagement	⟩ Meeting to review and accept deliverables ⟩ Final deliverables and SAMPLES

Notes:

1. Steps #1 Initiate engagement and #4 Create reports [Drafts AND Finals] all require deliverable acceptance for tw-Security to proceed to the next step.
2. During the evaluation assessment we will be mindful of other pertinent regulations and standards identifying gaps where apparent.
3. Services will be conducted remotely.
4. We will evaluate the existing risk analysis documentation, including assessments of biomedical devices.
5. During the evaluation, if our findings support creating new documentation, such as a policy/procedure, we will provide NMC with an estimate of the number of hours to complete. We anticipate this activity would occur after the evaluation during ISPS services.
6. The evaluation **does not include a technical evaluation** *(vulnerability scanning/penetration testing.)*

Copyright © 2020 tw-Security. ALL RIGHTS RESERVED. Confidential materials. Duplication or disclosure is prohibited without permission.

Cybersecurity, Data Privacy, and Compliance Program Support

Our information security/privacy support (ISPS) service is highly customizable; from providing advisory services to conducting strategic and tactical initiatives. Serving as your trusted advisor, we will provide support as needed with a deliverable focused "hands on" approach tailored for NMC.

The purpose of tw-Security's ISPS support service is to provide NMC with:

- An independent and broader view of information security, cybersecurity, and data privacy through the experience of a nationally known healthcare consulting firm and would now be familiar with NMC's programs, once we completed the evaluation as previously described
- Guidance to keep your security and privacy programs moving forward
  - Aid ongoing compliance efforts *(The HIPAA Security Rule and the Payment Card Industry Data Security Standard (PCI DSS) all require organizations to maintain their information security programs by periodically assessing risks and compliance gaps.)*
  - Risk remediation/risk management assistance to help manage risk to an acceptable level
  - A holistic approach to safeguarding protected health information (PHI) and personally identifiable information (PII) through evaluation, coordination, communication, and enhancement of the data privacy program
  - Support NMC's cybersecurity and data privacy strategy and program maturity
- Accountability to the corporate compliance committee and executive management
- Documentation of ongoing information security efforts (*Compliance and risk management are ongoing processes*)
- Knowledge to stay abreast of changes that impact your security program
- Cost effective, responsive access to experienced, certified professionals who are familiar with your organization, security and privacy program when needed
- Services inclusive of quality processes, oversight, methods and tools, supported by certified security and privacy professionals

Our approach is summarized below:

- **We prioritize tasks:** Our methodology assures that your limited resources are being applied where they are most needed: to address risk or compliance issues
- **We provide expertise when needed:** Through our ISPS services, we provide help as needed through emails or scheduled calls
- **Our tools are designed to be efficient and effective:** We have developed policies, procedures, and plans to align with multiple industry and regulatory requirements, tailored for each organization

Our process includes scheduled meetings *(agenda and minutes)* to document evidence of risk management. For each meeting, we track agreed to action items to ensure commitments are kept and progress is being made.

Copyright © 2020 tw-Security. ALL RIGHTS RESERVED. Confidential materials. Duplication or disclosure is prohibited without permission.

Approach Highlights

Communications: tw-Security will work closely with Ari Entin, Chief Information Officer, our point of contact and NMC's engagement liaison. If NMC desires, we will also work with NMC's law firm to ensure attorney-client privilege. tw-Security will maintain open communications to ensure that the services delivered meet your needs. We will notify you as soon as possible if we find any significant risks.

Confidential and sensitive information: Because our reports may document vulnerabilities and compliance gaps, these documents should be considered confidential and/or sensitive information. Also, these documents provide proof of compliance with HIPAA and therefore must be retained for six years. Our Report of Findings with recommendations will inform a prioritized action plan.

Project efficiency, discipline, and results: This engagement will be conducted in an efficient, cost-effective manner that does not compromise the quality of the engagement. tw-Security consultants are skilled at providing remote services. Our data gathering goes beyond checking a box on a checklist. We focus on the critical few rather than the trivial many. Some engagement activities require approval from NMC in order for tw-Security to proceed with the next step in this engagement. As such, NMC plays an important role in achieving a successful and efficiently managed engagement. Our methods and proprietary tools guided by tw-Security trusted advisors result in actionable deliverables which result in lower costs.

Project management: Regardless of the process being managed, the practice of good project management is a discipline. tw-Security aligns our project management practices and standards with the principles and methodologies of the Project Management Institute (PMI). Status progress and reporting, formal communications, and metrics are incorporated in our project management methodology.

Quality program: tw-Security monitors and measures the overall quality of our engagement delivery and customer satisfaction. We utilize our engagement management methodology to plan, deliver, verify, and conclude every engagement through a formal delivery oversight process. We monitor adherence to contractual obligations and quality standards to provide the highest level of service and customer satisfaction. Our quality processes are tightly integrated with tw-Security's Project Management methodology.

Copyright © 2020 tw-Security. ALL RIGHTS RESERVED. Confidential materials. Duplication or disclosure is prohibited without permission.

Deliverables and Timeline

Deliverables will be formally submitted for final review and approval. To avoid delays in the schedule and the associated increased cost due to slow deliverable review, deliverables not reviewed and approved or formally rejected with a cause in writing **within a review period of five (5) business days from delivery will be considered accepted.**

Based on the scope and approach outlined above, we estimate the HIPAA risk assessment engagement to be completed over a six to eight (6-8) week duration. tw-Security would be available to start the engagement within 15 days of contract signature provide **SOW is signed before January 1, 2021.** An engagement work plan will be developed and submitted for approval as part of the initiation activities.

The estimated engagement elapsed time is based on reasonable expectations of tw-Security and NMC's resource availability. *(Based on the actual availability of these resources, the schedule may be adjusted during the engagement.)*

Staffing

Our 'high availability' staffing model eliminates a single point of failure with multiple assigned resources and ensures a reliable crossover and participation in engagement activities. Our assignment process incorporates a weekly review to detect and resolve any staffing issue or challenge, in a seamless manner as we work behind the scenes on activities as an extension of your workforce.

All tw-Security consultants are skilled and experienced in following our risk assessment methodology, using propriety tools and templates. **Qualified consultant(s) will be assigned based on consultant availability.** Our consultants average more than 25 years of relevant experience and maintain critical certifications that best prepare them to provide our customers with superior service.

tw-Security reserves the right to utilize multiple resources to deliver a quality engagement. tw-Security stands behind all its work meeting or exceeding contractual obligations and customer expectations. Please see profiles of our team at https://www.tw-security.com/about-us/our-leadership-team.

Tom Walsh, Founder and Managing Partner, tw-Security, will serve as the Project Executive Sponsor. As the Project Executive, Tom is responsible for championing the engagement and ensuring that all tw-Security resources are available to ensure that the engagement is a success. The Project Executive is the final escalation point and decision-maker for all engagement issues.

Additional Projects and Change Order Process

Projects, remediation activities, or tasks can be addressed throughout the term of the contract as needed when mutually agreed upon through a separate SOW, Change Order or a Professional Services Agreement documenting our good faith estimates associated with those changes for consideration and approval.

tw-Security's projects have a defined scope with clear start/finish and tasks/deliverables and generally, require a level of effort of 10 or more hours. Work effort on any change or new project will not begin until the request is reviewed with NMC and mutually agreed upon in writing.

Copyright © 2020 tw-Security. ALL RIGHTS RESERVED. Confidential materials. Duplication or disclosure is prohibited without permission.

Critical Success Factors

A successful engagement depends on trusting relationships and mutual considerations.

tw-Security will:

- Work with NMC to determine the engagement plan, specific tasks, resource estimates, schedule and coordination of any activities; NMC's engagement liaisons will have final approval authority
- Submit deliverables for customer review and approval
- Provide timely responses to emails and calls, typically within one to two business days
- Ensure that the quality of work provided meets the standards set by NMC *(Any rework required to resolve unacceptable work will be done at no additional cost.)*
- Periodically assess NMC's overall satisfaction with the engagement

NMC will:

- Assign a liaison to serve as a focal point with the responsibilities of reviewing and providing feedback of documentation submitted and resolution of engagement issues
- Provide tw-Security with all relevant policies, procedures, standards, plans, forms, etc. for review
- Ensure timely and effective communication will occur between NMC key personnel and tw-Security
- Send meeting invites to engagement participants and participate in scheduled meetings/calls
- Remain actively engaged and make the appropriate commitment of time necessary to keep the engagement moving forward according to the engagement plan
- Provide feedback and maintain open communications with tw-Security as the engagement progresses so that adjustments can be made as needed
- Provide access to internal resources which would reasonably be required to successfully carry out this SOW, including the documents requested, names and contact information of staff, etc.
- Provide administrative assistance if needed *(tw-Security will try to minimize the need for administrative assistance from NMC staff.)*

Other assumptions:

- tw-Security cannot guarantee or certify that NMC will be HIPAA compliant as a result of this engagement (*Only the US Federal government can officially declare an organization "compliant."*)
- The management of NMC is responsible for establishing and maintaining effective internal control over compliance with the requirements of laws, regulations, contracts, and grants applicable to programs funded through the federal government
- Actual changes to processes and systems will not be formally made as part of this engagement *(Recommendations will be made to those responsible for the affected processes and systems. Where feasible, the action plan will have rough estimates of the resources and time commitments required.)*
- tw-Security will not be held responsible for the accuracy of information provided to tw-Security by any of the interviewees
- Beyond HIPAA, there is other confidential information vital to the organization that also needs to be protected. A "HIPAA centric" approach would likely not include other types of confidential information in a risk analysis. Therefore, just meeting the HIPAA Security Rule does not translate to a secure environment.

Copyright © 2020 tw-Security. ALL RIGHTS RESERVED. Confidential materials. Duplication or disclosure is prohibited without permission.

Professional Fees and Expenses

Our philosophy is to establish long-term relationships with our customers. We believe the best way to do this is to provide consulting services that not only provide value but also are delivered with concern for your budget. We provide only those services that you specifically require, with professional fees that reflect our consultants' experience and ability to produce results. In addition, we make a conscious effort to keep out-of-pocket expenses to a minimum.

Professional Fees

We are providing good faith estimates (GFE) of hours and fees. We track actual hours worked, plus any out of pocket expenses. Hourly rates are rounded to the nearest quarter hour. Professional services will be billed according to the schedule below:

- $250/hr. for offsite discretionary time (DT) which are tasks that are not constrained by a specific deadline for completion, rounded to the nearest quarter hour
- $275/hr. for onsite, emergency, afterhours, and On-Demand support

Note: *Because incidents and cyber-attacks can occur at any time, emergency and afterhours support by our team of certified security professionals falls within the On-Demand support model.*

Note: *Meeting 'no-shows' will result in a 15-minute professional fee charge.*

Services	Estimated Hours	Estimated Fees
HIPAA and Cybermaturity Programs Evaluation	125 – 135	$31,250 – $33,750
Information security/privacy support	100 "bucket of hours"	$25,000

Notes:

1. **Amount not to exceed of $68,750, including travel for contract term January 1, 2021 through December 31, 2021**.
2. **There is no minimum or retainer for** Information security/privacy support services
3. **If NMC establishes a budget of hours or cost, we will prioritize activities and monitor the usage to ensure that we stay within those parameters.** *We will work with NMC to determine the appropriate schedule that will best meet your needs and budget.*
4. If travel is involved, our preference is to provide a minimum of two consecutive days when onsite.

Expenses

In addition to the professional fees, tw-Security shall invoice for all reasonable out-of-pocket expenses incurred by tw-Security personnel. Out-of-pocket expenses are any reasonable expenses incurred in the performance of the services as described in the Master Agreement. tw-Security will make every effort to reduce expenses when possible throughout the course of the engagement.

All travel expenses shall be reimbursed by NMC to tw-Security in accordance with the County of Monterey Travel and Business Expense Reimbursement Policy (Exhibit B).

Copyright © 2020 tw-Security. ALL RIGHTS RESERVED. Confidential materials. Duplication or disclosure is prohibited without permission.

Confidentiality and Non-Disclosure

NMC acknowledges that, while performing work with tw-Security, its employees and other members of its workforce may acquire knowledge or information considered by us to be confidential or proprietary. tw-Security confidential information means information we disclose to NMC either orally or in electronic or written forms identified as “confidential” or “proprietary.” NMC will not publish or disseminate to any party, other than its employees or independent contractors with a need to know any tw-Security Confidential Information. NMC agrees that tw-Security may acknowledge that NMC has engaged tw-Security for consulting services.

Ownership of Materials

All materials, including any documentation and reports created under the SOW, will belong to both parties. Each party retains the right to copy and use the materials developed during this engagement in its business without the other party’s consent if no such use violates the confidentiality provision stated in the SOW.

Any materials first produced by tw-Security outside of this engagement, even if the materials were incorporated under the SOW, remain the exclusive property of tw-Security, but may be used by NMC as incorporated in the materials, but not separately. Further, tw-Security may create for itself or others materials which, are like those materials created for NMC under the SOW if no such use violates the confidentiality provision.

Thank you!

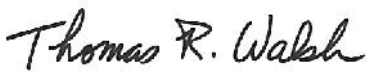
We appreciate the opportunity to submit our SOW and look forward to the possibility of working with you on your information security initiatives. We are hopeful that you find the approach articulated in this SOW responsive to your needs and expectations. If you have any questions regarding the specifics of our SOW, we can be reached by telephone at **913-696-1573** or by email at **tom.walsh@tw-Security.com**.

Acceptance

Natividad Medical Center and tw-Security acknowledge that this statement of work for HIPAA Programs Evaluation and support services is executed in accordance with and is subject to the terms and conditions of the Master Agreement. In the event of a conflict between the provisions of the Master Agreement and the provisions of this statement of work, the provisions of the tw-Security Standard Agreement shall control.

Upon authorization, tw-Security will schedule staff to begin this engagement based on mutually acceptable schedules. Unless executed by signature below, this proposal will expire in 45 days. Natividad Medical Center’s acceptance of this proposal is indicated by signing below and **returning the Acceptance of Proposal section**, becomes the complete and binding Agreement.

Sincerely,



Thomas R. Walsh
Founder and Managing Partner, tw-Security
Date: December 1, 2020

Copyright © 2020 tw-Security. ALL RIGHTS RESERVED. Confidential materials. Duplication or disclosure is prohibited without permission.

Appendix A: Why tw-Security?

- Experienced consultants: All of our consultants have either served as a healthcare Chief Information Security Officer (CISO), Privacy Officer (PO), or have functioned *(or are currently functioning)* in an interim CISO or PO for a large healthcare system or academic medical center. We are experienced with implementing regulatory requirements and industry standards. In contrast to firms who only provide assessments, tw-Security actively assists multiple customers to guide and develop, monitor and maintain, and improve their HIPAA and cybersecurity programs through hands-on support and ongoing advisory and managed services. **There are no junior consultants on our staff**.
- Experience and approach: We understand the 'intent' of the HIPAA Security Rule having the good fortune to work side by side for multiple years with John Parmigiani, the former Director of Enterprise Standards, Health Care Financing Administration (HCFA), currently known as The Centers for Medicare & Medicaid Services (CMS), immediately after he left the USA federal government. John was directly instrumental in the creation of the HIPAA Security Rule. We have conducted hundreds of risk assessments and risk analysis; therefore, our processes are well-defined.
- Performance excellence: In January 2020, an impartial healthcare research firm announced cybersecurity advisory vendors rankings across customer experience pillars. In the report, tw-Security came in second! narrowly missing the top spot with a scored 95, we try harder! Representing data collected since 2018, we received an A-plus rank in loyalty (*would buy again, overall satisfaction, and likely to recommend.)* We also received A-grades in operations, relationship, and value, and an A-minus in services.
- Methodology: Our risk analysis methodology is based upon the guidance from National Institute of Standards and Technology (NIST) and documents created by the Department of Health and Human Services (DHHS) and/or the Centers for Medicare and Medicaid Services (CMS). *All of tw-Security's customers that have undergone an audit by the Office for Civil Rights (OCR) or Figliozzi and Company (contractor to CMS) have passed the core measure for risk analysis, the most critical requirement of the HIPAA Security Rule.*
- Tools and deliverables: Our tools scale and are tailored to accommodate small providers to a large health system, academic medical center, and business associates. Our method for compliance assessments is to focus on those critical items repeatedly cited in the OCR settlement agreements and the corrective action plans (CAPs) as a means for prioritizing efforts to close compliance gaps. Our deliverables are easy to read and follow and we provide mentoring on how to use the tools, making our customers more self-sufficient.
- Relationships: We strongly believe in long term relationships with customers; the majority of our customers have been working with us for seven or more years.
- Staffing model: We balance onsite and offsite activities for efficiency and productivity. We assign multiple resources to eliminate a single point of failure. Our staff are experienced credentialed consultants committed to this engagement who are trained on and use tw-Security's methods and tools. We incorporate a weekly review to detect and resolve any staffing issue or challenge.
- Project management: tw-Security aligns our project management practices and standards with the principles and methodologies of the Project Management Institute (PMI).
- Stability: tw-Security is a privately held, vendor-neutral, partner-owned company with a solid balance sheet and a track record of controlled growth that has enabled it to nurture its customer relationships over the long term.

Copyright © 2020 tw-Security. ALL RIGHTS RESERVED. Confidential materials. Duplication or disclosure is prohibited without permission.

Exhibit B

TRAVEL AND BUSINESS EXPENSE REIMBURSEMENT POLICY

Revised December 11, 2012

TABLE OF CONTENTS

I. PURPOSE

The purpose of this policy is to establish uniform travel and business expense reimbursement policies, rules and claim procedures for persons authorized to conduct County business.

II. SCOPE

The County travel and business expense reimbursement policy applies to all County employees, members of legislative bodies established by the Board (salaried or not), non-County employees (such as contractors who receive travel and/or business expense reimbursements) and volunteers traveling on County business.

III. DEFINITIONS

Unless the context otherwise requires, the definitions contained in this part govern the construction of this policy. They do not necessarily apply in other County contexts.

A. Accountable Expense Reimbursement Plan

Reimbursements of travel and other business expenses to a County employee, contractor or volunteer will be considered to be made under an "Accountable Expense Reimbursement Plan" if the following three requirements are met:

- The person substantiates his or her expenses by submitting an expense report with
  1) the amount of the expenditure,
  2) the time and place of the travel or business entertainment,
  3) the business purpose of the expenditure, and
  4) the names and business relationship of any persons entertained.
- The person documents the expenses with supporting receipts, paid bills, etc. within 60 days after the expense is paid or incurred, and
- Excess advances, if any, are repaid to the County within 120 days after the expense is paid or incurred.

"County" means the County of Monterey.

B. County Business

"County business" means the activity directly related to the ordinary, necessary and/or required business functions of the County of Monterey ("County"). It does not include travel or expenses related to an employee's participation in the County's Educational Assistance Program or commuting expenses (a non-reimbursable expense).

C. County Employee

"County employee" means any County officer or employee, whether elected or appointed, filling a budgeted position approved by the Board of Supervisors.

Independent contractors and their employees are not County employees.

D. County Traveler

"County traveler" means any County employee, authorized non-County employee (such as a contractor) or volunteer traveling on County business. Agency temporary employees are not covered by this policy and are not reimbursable for travel.

E. County Volunteer

"County volunteer" means a person, other than a County employee, who performs volunteer work authorized by a department or the Board of Supervisors for the County, such as a department volunteer, a commissioner or a member of an interview panel. It does not include agency temps, inmates, wards or probationers working for the County.

F. Home

"Home" means the actual dwelling place of the County traveler without regard to any other legal or mailing address.

G. Main or Regular Place of Work

"Main or regular place of work" means the principal place of business for the County employee or the principal location to which the County volunteer/contractor is assigned to work for the County. This may be the place at which s/he spends the largest portion of his/her regular County workday or working time or, in the case of field workers, the assigned location/headquarters to which s/he returns upon completion of regular or special assignments.

H. Meals

Meals that are 1) directly related or associated with bona fide County business matters and 2) approved for reimbursement by a member of the Board of Supervisors or a department head (or his or her designee) will be considered a reimbursable County business expense, if incurred in connection with out-of-County business travel or while conducting in-County business. Also, reimbursement for the provision of in-kind meals to employees on the business premises of the County will only be allowed if there is a substantial non-compensatory business reason for providing such meals to employees.

I. Temporary Work Location

"Temporary work location" means the place where the County employee, volunteer or contractor is assigned on an irregular or short-term basis. If an employee is assigned to a work location for no more than 35 work days during a calendar year, then the location is considered temporary. Attending conferences, meeting or training sessions away from the main or regular place of work by County employees or volunteers, or field

workers conducting fieldwork at off-site locations, does not normally constitute assignment to another site. If the employee is assigned for more than 35 work days during the calendar year, the new location has become the main or regular place of work.

J. Vehicle

"Vehicle" means a motor vehicle, which can be legally operated on public highways.

IV. AUTHORIZATION TO TRAVEL

A. General Conditions

1. Travel will be authorized only when the travel is necessary and in the best interest of the County.

2. Advance authorization is required for all County travel, as specified in B & C.

3. Advance written authorization from the County Administrative Officer is required for all County travel by County volunteers, except as follows:

   a) Travel by appointed members of County boards, commissions, or advisory committees to and from the official meetings of their respective boards.

   b) Travel to and from the County for members of personnel interview panels, subject to authorization by the Human Resources Department.

   c) Travel to and from meetings, conferences and training covered by the County MHSA plan, subject to authorization by the Behavioral Health Program Manager or designee.

B. In-County Travel

County employees are authorized to travel within the County when said travel is required by the department and is considered a part of the routine, day-to-day official duties of the employee as defined and authorized by the department head or his/her designee. All other in-County travel requires advance authorization by the department head or his/her designee.

C. Out-of-County Travel

1. All travel outside of the County, but within the State of California, requires advance authorization by the department head, or his/her designee. Travel by immediate staff of a member of the Board of Supervisors requires the advance authorization of the respective Board member.

2. All travel outside of the State of California requires advance written authorization by the department head, or his/her designee. Travel by immediate staff of a member of the Board of Supervisors requires the advance authorization of the respective Board member.

3. Authorization for out-of-state travel by current members of the Board of Supervisors is subject to the guidelines established by the Board.

D. Travel Requests

Travel requests that require department head authorization shall be submitted to the department head pursuant to department policy. If the traveler is requesting a travel advance, an approved "County of Monterey Travel Request" form (usually in the form of a “white claim” or “GAX”), accompanied by all documentation relative to the request, shall be forwarded to the Auditor-Controller.

V. TRAVEL EXPENSES

A. General Conditions

1. County travelers are entitled to submit a claim for actual and necessary expenses for transportation, meals, lodging, and incidentals for authorized travel, subject to the conditions set forth in this Travel and Business Expense Reimbursement Policy (“Policy”), whenever the expenses are incurred as part of his/her official duties and authorized because the County traveler is required to work, attend a school, training, meeting or convention overnight at a location sufficiently distant from main or regular place of work to qualify under this policy for meal per diem and overnight lodging.

2. Notwithstanding Section 1 above, claims shall be paid subject to the rules set forth in this Policy and statutory law. Eligibility to submit a claim does not automatically entitle the claimant to reimbursement for any and all expenses.

3. County travelers receiving reimbursement from an outside source for travel on County time shall forward said reimbursement to the County Auditor-Controller for handling and deposit if the traveler intends to submit an expense claim to the County or use County resources to travel. Said travelers shall then be entitled to submit a claim for actual and necessary expenses for transportation, meals, lodging, and incidentals, subject to the conditions set forth in this travel policy.

4. Arrangements for transportation, lodging or registration fees that have cancellation or change penalties shall be carefully monitored by the department. If cancellation/change occurs due to direction by the County traveler's department head, or his/her designee, or the County Administrative Officer, the County department will cover the penalty cost. If the cancellation/change occurs due to a traveler's personal request or obligations, the traveler will be required to pay the

penalty. Exceptions shall be made when a traveler is unable to travel because of hospitalization, serious sickness or death of self or an immediate family member or when the department head certifies that the reason for the employee's absence was legitimate and authorized.

B. Transportation Expenses

1. General Conditions

   a) Transportation expenses are the direct costs related to movement of the County traveler from authorized point of departure to destination of travel and back to the authorized point of return.

   b) All transportation expenses incurred shall be based upon the most efficient, direct, and economical mode of transportation required by the occasion.

   c) Whenever a time frame is established as criteria for eligibility for claiming, such as the requirements set forth for meals in Section V, subsection C. 1. d., estimated travel time shall be based upon legal vehicle speed limits, volume of traffic, and weather conditions in effect at the time of travel.

2. Vehicle Transportation

   Vehicle use (both County-owned and private) by authorized County travelers during the conduct of official County business is subject to the County Vehicle Use Policy.

   a) Private Vehicle

      (1) Travel by private vehicle will be reimbursed at the IRS rate for business use of a personal vehicle in effect in the County at the time of travel.

      (2) Authorized County travelers who travel in a vehicle other than their own may not claim mileage for business use of a private vehicle but may claim reimbursement of actual fuel expenses necessary for the trip and expended by the traveler. Receipts are required and should be claimed by the employee actually paying the expense.

      (3) Authorized County travelers may not claim mileage for business use of a private vehicle in the following instances:

         (a) when the County traveler is riding with someone who will be claiming reimbursement for the vehicle's use from the County or another source;

         (b) when the County traveler is traveling in a County or other government

agency vehicle;

(c) when the County traveler is traveling in a rented vehicle (paid by County);

(d) when the County traveler has been assigned a County Vehicle for home retention, is receiving an allowance or lump sum for mileage, unless specifically provided for in the terms of their agreement or contract with the County or by Board resolution.

(4) County employee mileage to the regular or main place of work from home, and back, is considered commuting and may not be claimed.

(5) County employee mileage to the temporary work location from home, and back, is considered commuting and may not be claimed except in the following cases:

(a) if the County employee is required to report to the regular or main place of work before reporting to the temporary work location, s/he is eligible for mileage from the regular or main place of work to the temporary work location;

(b) if the County employee is required to report to the regular or main place of work after working at the temporary work location and before going home, s/he is eligible for mileage from the temporary work location to the regular or main place of work.

(6) Mileage in conjunction with authorized County travel to and from a school, training, convention or meeting shall be based on the distance to the destination from the traveler's home or the regular or main place of work, whichever is less, except in the following cases:

(a) if the traveler is required to report to his/her work location before leaving, s/he is eligible for mileage to the school, training, convention/meeting from the work location.

(b) if the traveler is required to report to his/her work location before returning home, s/he is eligible for mileage based on the distance from the school, training, convention/meeting to the work location.

(7) Appointed volunteer members of County boards, commissions, or advisory committees may claim mileage to the official meetings of their respective boards from home, and back.

(8) Members of personnel interview panels may claim mileage to the panel location from their regular or main place of work, and back.

(9) When two or more County travelers from the same department are traveling to the same site by vehicle, they should use only as many vehicles as are required to accommodate the number of travelers and business needs of the County. If a County traveler chooses to use a separate private vehicle because of personal preferences or obligations, h/she shall not be eligible for mileage or fuel reimbursement for the travel unless the department head determines that reimbursement is appropriate and justified.

(10) If a County traveler chooses to use a private vehicle instead of an alternative mode of transportation chosen by the department head because of personal preferences or obligations, his/her mileage reimbursement shall not exceed the cost of using the alternative mode of transportation unless the department head determines that the additional reimbursement is appropriate and justified.

b) County Vehicle Transportation

(1) County travelers using a County vehicle for traveling shall not be eligible for reimbursement for mileage.

(2) County travelers required to fuel a County vehicle at their own expense should claim the actual fuel costs expended by them. Receipts must accompany the claim. Vehicle license number and the odometer reading should be written on the receipts.

(3) If the County vehicle experiences mechanical failure, the County traveler shall follow the rules set forth in the "Mechanical Failure" section of the "Vehicle Operator's Handbook" located in the glove compartment of each County vehicle.

c) Rental Vehicle Transportation

(1) Vehicles may be rented for transportation at the destination point when the County traveler travels to the destination via commercial common carrier and the cost of the rental will be less than the charge for shuttle or taxi service to and from the carrier termination point to the function or hotel accommodations.

(2) Vehicles may be rented for transportation to the destination point when the cost of the rental will be less than other reasonable and available modes of transportation.

(3) If more than one County traveler from the same department is traveling to the same function, only one rental vehicle may be claimed and then only if

it is available for use by all of the County travelers.

(4) The County traveler shall choose the least expensive size and mileage limits appropriate to the use required. Rental expenses for luxury cars, motorcycles and recreational vehicles may not be claimed.

(5) Rental cars shall be refueled prior to return to the rental agency to reduce cost to the County. Rental cars should be returned to the renting location and on time to avoid additional charges.

(6) When traveling domestically the County traveler shall waive additional vehicle insurance (except for additional driver and coverage for drivers under 25 years of age), provided that the employee has his/her own vehicle insurance coverage. When traveling internationally additional insurance should be accepted if the traveler lacks other similar coverage.

(7) An original car rental receipt showing the number of days and type of vehicle rented is required for vehicle rental claims. A copy of the receipt or a credit card receipt alone is insufficient.

d) Commercial Carrier Transportation

(1) County travelers shall seek and attempt to use the lowest rates available for the type of commercial carrier service being utilized. Whenever possible, travelers should take advantage of flight arrangements that minimize County cost (for example, purchasing a round trip ticket may be less expensive than two one-way tickets). Reservations should be made as far in advance as possible to take advantage of available discounts and special offers. Travel agents that have added ticket handling charges should be avoided.

(2) Claims for travel via commercial carrier shall be limited to the cost of travel at economy rates for the same day and time of travel or actual cost, whichever is less. County travelers may upgrade tickets, provided that the traveler and not the County pay for the difference in cost for such upgrade. The County will not reimburse any type of travel insurance unless the Department Head requests the traveler to purchase cancellation coverage. Reasonable baggage charges, if imposed by the airline, on the first checked bag are reimbursable.

(3) Claims for commercial carrier tickets shall be substantiated by an original ticket document (such as an e-ticket or passenger receipt ticket copy) showing the price, date, date/time of travel and class of travel. A copy of the credit card receipt or statement from a travel agency alone is insufficient.

(4) County business traveler may retain frequent flyer/hotel rewards and similar program benefits. However, participation in these programs must not influence flight/hotel/etc. selection, which would result in incremental cost to the County beyond the lowest available airfare/hotel cost unless the difference is paid by the traveler. Free tickets or cash allowances for volunteering to be denied timely boarding may be retained by the traveler but no additional cost to the County or interruption of County work is allowed and any additional time required to complete the trip is to be personal time.

(5) Should a Saturday night stay reduce the cost to the County of a ticket more than the total of any additional hotel/meal/parking cost, the costs to do so are reimbursable to the traveler but should be well-documented with a clear savings to the County.

e) Private Aircraft Transportation

(1) Traveling by private aircraft which is flown by a County employee may be authorized if it will be the most efficient means of travel and the flight is incidental to the purpose of the County travel. Said use shall require the advance written approval of the County Administrative Officer. If approved, the following must be provided to the Auditor-Controller's Office in advance of the travel:

(a) a copy of the pilot's Federal Aviation Administration (FAA) pilot's certificate and instrument rating for the category and class of aircraft to be flown and the type of flying to be performed;

(b) a copy of the pilot's current medical certificate;

(c) a copy of the FAA Pilot Proficiency Award Program certificate issued to the pilot within the twelve months prior to the flight;

(d) a copy of the pilot's flight log showing a minimum of 250 hours of flight time within the twelve months prior to the flight;

(e) a certificate of public liability and property damage insurance of not less than $1,000,000 naming the County as an additional insured.

(2) Traveling by private aircraft, which is flown by a non-County employee, except for flights conducted by members of the Sheriff's Air Squadron in the performance of their official duties, is normally prohibited.

(3) County travelers who operate a private aircraft in connection with approved County travel may be reimbursed the actual cost paid by the

traveler for fuel used by the aircraft on the trip or the County's mileage rate for each air mile at the travelers option.

f) Other Transportation Expenses

(1) The following necessary transportation expenses may be claimed at actual cost (receipt required) when directly related to transporting the County traveler to and from the business destination point:

(a) taxi, shuttle, or public transit fares;

(b) parking fees (airport long-term parking is required for travel exceeding 24 hours);

(c) bridge, road or ferry tolls;

(d) other actual transportation expenses determined to be reasonable and necessary by the department head and the Auditor-Controller.

(2) The following transportation expenses may not be claimed:

(a) traffic and parking violations;

(b) emergency repairs or non-emergency repairs on non-County vehicles;

(c) personal travel while at an out-of-County location;

(d) other actual transportation expenses determined to be unreasonable or unnecessary by the department head or the Auditor-Controller.

C. Meal Expenses

1. Eligibility for Meals

a) County employees, contractors and volunteers may be reimbursed for in-County meal costs that are 1) ordinary (not extravagant) and necessary, 2) directly related or associated with bona fide County business matters and 3) approved by a member of the Board of Supervisors or a department head (or his or her designee). County business discussions associated with a meal must be conducted in a “clear business setting”.

b) County travelers involved with in-County travel that does not require an overnight stay away from their home are not eligible to claim for meals taken outside the County, unless the requirements of paragraph a) above are met, or unless provided for in a Board of Supervisor-approved written County policy.

c) County travelers on out-of-County business travel that requires an overnight stay away from their home are eligible to claim for meals taken out-of-County.

d) County travelers are eligible to claim the meal reimbursements noted below for travel requiring overnight lodging if the total travel time (work time, plus the lunch period plus round-trip travel time) is estimated to equal or exceed 12 hours.

(1) Breakfast may be claimed if the County traveler must reasonably be away from home because of County business travel at or before 7:00 a.m.

(2) Lunch may be claimed if the County traveler must reasonably be away from home because of County business travel at or before Noon.

(3) Dinner may be claimed if the County traveler must reasonably be away from home because of County business travel at 7:00 p.m. or after.

e) Snacks are a personal expense, not reimbursable.

f) Claims for meals purchased by a County employee or volunteer on behalf of federal, state or local public officials or employees is prohibited, including any other Monterey County employees, unless provided for under other Board of Supervisor approved written County policies.

g) County travelers are not eligible to claim meals or other expenses for those persons who are not otherwise eligible to file a claim themselves for County reimbursement.

h) County travelers are not eligible to keep or claim per diem allowances for anyone other than themselves.

2. Meal Claims

a) The County maximum full day meal and incidental expenses rate shall be equal to the maximum federal per diem meal and incidental expenses (M&IE) rate established by the GSA. Said maximums include taxes and gratuities.

b) Meal expense amounts shall be calculated by the Auditor-Controller for first and last partial days of travel based on the maximum federal per diem meal rate for the appropriate meal(s).

c) Claims for out-of-County meals taken in conjunction with travel that includes an overnight stay away from the traveler's home shall be reimbursed in the form of a "per diem allowance", which means the traveler is eligible to be reimbursed at the maximum rate allowed and receipts are not required (except for Board of

Supervisor Members). Partial days shall be reimbursed at the appropriate meal rate.

d) Allowable meal costs may only exceed the prescribed per diem rates if the meal is being served at a conference or workshop and the costs of the speaker, conference, and/or registration are included in the price. The agenda/brochure or other documentation describing the event and the price must accompany the claim to the Auditor-Controller's Office.

e) A County traveler may not claim a per diem allowance or reimbursement for any meal which is provided, or otherwise available, to the County traveler with the lodging or function, whether or not there is an actual charge for the meal. For example, if lunch is provided at the function or breakfast is included in the cost of lodging, the traveler may not claim a per diem allowance or request reimbursement for eating elsewhere. For purposes of this section, continental breakfast and meals provided during airline or other commercial carrier travel do not constitute provided meals and do not need to be deducted from the per diem allowance. A County traveler may not claim a per diem allowance for a meal that was paid for by someone else.

f) If a breakfast is included in the cost of lodging, the traveler may not claim for a breakfast meal; however, s/he may apply the next day's breakfast allowance amount towards the maximum lodging amount. For example, if the maximum lodging amount is $79.00 and the breakfast allowance is $8.00, the employee may claim up to a maximum of $87.00 for lodging which includes a continental breakfast. (For purposes of this section, continental breakfast does not constitute a provided breakfast meal.)

g) Claiming for alcoholic beverage expenses are prohibited in all cases.

h) As required by California Government Code 53232.2 Board of Supervisors members must provide receipts for all meals and will be reimbursed at the lower of the appropriate per diem amount or the actual expense.

D. Lodging Expenses

1. Eligibility for Lodging

a) County travelers are not eligible to claim for lodging for in-County functions.

b) For out-of-County business that is conducted on one business day, if the County traveler’s actual time for the day is estimated to equal or exceed 12 hours (including work time, the lunch period and round-trip travel time), then the County traveler will have the option of securing one night’s lodging at either the

front-end or back-end of the trip. Illustration: A member of the County Board of Supervisors who resides in Monterey County is required to attend a one-day business meeting in Sacramento. The Board member estimates that his total time for the day without obtaining lodging would be 14 hours (8 hours of meetings, 1 hour for lunch and 5 hours for round-trip travel). The Board member will have the option of securing one night's lodging in Sacramento, either the night before the meeting, or after conclusion of the meeting.

c) For out-of-County business that requires multiple business days, if County travelers are eligible to claim lodging for the first and last evenings of an out-of-County trip, they are also eligible to claim lodging for any evenings that fall in between the first and last evenings of the trip.

d) County travelers are not eligible to claim reimbursement of lodging costs when staying overnight as a guest of friends or relatives.

2. Lodging Claims

a) Lodging expenses shall be claimed at either the actual cost of the lodging (limited to the single occupancy rate for a single room) or the County's maximum lodging rate (Federal Per Diem Rate), whichever is less. Receipts are required. Taxes are in addition to the Federal Per Diem Rate.

b) Lodging costs may exceed the County's maximum lodging rate only when a conference, meeting or convention is being sponsored by an organization of which the County, the department or employee is a member, the lodging may be claimed at the actual cost if seminars or meetings are to be held at the particular hotel and/or events are scheduled for evening hours, and the department head has given advance written authorization.

c) An original room folio receipt, showing the number of days and the number of occupants, is required for lodging claims. A copy of the receipt, travel agency statement or a credit card receipt alone is insufficient.

d) When a room is shared with a fellow County traveler, the expense may either be prorated, and the prorated amount claimed by each County traveler, or one County traveler may claim the total expense at the multiple occupancy rate.

e) When a room is shared with a person other than a County traveler and said person will also be claiming reimbursement from the County or another source, the amount shall be prorated between the two travelers.

f) Lodging expense may not be claimed for guests of the County traveler. Where expense for a family member or friend is included in the receipt, the claim must not exceed the single occupancy rate.

g) Special lodging, such as accommodations in apartments, RV parks, campgrounds or other semi-permanent lodgings, shall require advance written authorization of the County Administrative Officer and the Auditor-Controller.

h) County travelers should inquire when making lodging arrangements whether the County is exempt from Transient Occupancy Taxes (TOT) in the locale where they are staying and should provide the necessary form to the lodging facility, if required to do so to obtain the waiver.

h) Except when registering for lodging at a pre-arranged group rate in conjunction with a conference or meeting, County travelers shall request the government rate or lowest available eligible rate when making lodging arrangements.

i) Travelers are responsible for canceling hotel rooms before the cancellation period ends and should record the cancellation number in case of disputes. Travelers will not be reimbursed for "no-show" hotel charges unless there are unavoidable reasons for not canceling the room.

j) When multiple country travelers are traveling together and the rooms are put on one invoice, one traveler may take care of the invoice but should provide the details on who stayed in each room on the invoice.

E. Registration Fees

Conference, convention and seminar registration and tuition fees may be claimed at the actual cost, provided that the agenda/brochure or other documentation describing the event, including the price, accompanies the approved claim to the Auditor-Controller's.

F. Other Travel Expenses

1. County travelers are eligible to claim a per diem incidental allowance, limited to the maximum federal per diem incidental rate established by the IRS, for each day of travel requiring an overnight stay away from the traveler's home. Said allowance covers fees and gratuities for persons who provide services, such as food servers and luggage handlers, and does not require receipts (Except for Board of Supervisors Meals). If applicable (such as a Board of Supervisor meal), gratuities are limited to not exceed 15% of the service costs unless billed by a provider's standard policy at a higher rate.

2. County travelers are eligible to claim the following expenses at actual cost, even if they also qualify for a per diem incidental allowance. Receipts are required.

   a) County business calls (traveler must annotate purpose of call on the bill)

   b) fax machine charges incurred to send or receive documents for County use.

c) copy machine charges incurred to copy documents for County use.

d) Internet access connection and/or usage fees away from home not to exceed $15.00 per day, if Internet access is necessary for county related business.

e) other business related expenses determined to be reasonable and necessary by the department head and the Auditor-Controller.

VI. OTHER COUNTY BUSINESS EXPENSES

A. General Guidelines

In the course of conducting County business, employees, contractors or volunteers may incur business expenses (including meal expenses pursuant to Section V.C) on behalf of the County. Such expenses will be approved for reimbursement if the disbursement meets the following requirements:

- The disbursement is for an ordinary (not extravagant) and necessary expense of conducting County business, or is an expense that is required by the County,
- The expense is approved by a member of the County Board of Supervisors, or a County department head (or his or her designee), and
- The payee accounts for the expense in accordance with the rules for a "Accountable Expense Reimbursement Plan", as set forth in the Internal Revenue Code and related regulations.

B. Taxation of Business Expense Reimbursements

If a reimbursement to an employee, contractor or volunteer meets the requirements of an "Accountable Expense Reimbursement Plan", then such reimbursement will not be reportable for federal or California income tax purposes.

VII. CLAIMING PROCEDURES FOR OUT-OF-COUNTY TRAVEL

A. Travel Advance Claims

1. Authorizations and Eligibility

a) Travel advances are strongly discouraged and are only available to County employees. The issuance of travel advances creates double work for departmental and auditor-controller staff and should only be used if a County travel card cannot be used or the employee does not have a personal credit card. Board of Supervisors Members are not eligible for travel advances.

The first choice is for travelers to use their personal credit cards to pay for their

travel expenses and be reimbursed before their monthly statement arrives. Secondly, the County has arranged for the use of the Travel Card to pay many travel related expenses. Departments may use their Travel Cards to pay for airline tickets and conference registration expenses for all of their employees, not just the cardholder. Commercial carrier and conference registration expenses should not be considered in the advance calculation. The third choice would be a cash advance, if necessary.

b) Travel advances require the authorization of the department head or his/her designee, and the Auditor-Controller or his/her designee.

c) The net amount of the travel advance shall not exceed the following:

(1) 75% of the total estimate for the following travel expenses, exclusive of payments made payable directly to the vendor:

(a) lodging (documentation, including at least the confirmation number and hotel name should be provided), including hotel parking

(b) rental vehicle transportation;

(c) per diem meal allowances;

(d) long-term airport parking;

(e) other out-of-pocket expenses deemed necessary and reasonable by the Auditor-Controller.

(2) 50% of the total estimate of reimbursement for mileage for business use of a private vehicle.

d) A travel advance shall not be issued for a net amount less than $100.00 nor more than $2,000.00.

e) A travel advance shall not be issued more than thirty (30) calendar days in advance of the commencement of travel.

f) Travelers are not eligible for an additional travel advance if they have an unsettled advance, unless the advances are for travel taken consecutively. In such case, the sum total of the travel advances shall not exceed $2,000.00.

2. Travel Advance Requests

a) Requests for travel advances involving travel shall be submitted by the department head to the Auditor-Controller's Office on a completed and signed

"County of Monterey Travel Request" form, accompanied by all documentation relative to the request, at least ten (10) working days in advance of the commencement of travel.

b) After a completed and approved "County of Monterey Travel Request" form is received by the Auditor-Controller's Office, a warrant payable to the County traveler for the amount requested shall be issued, up to the 100% maximum amount allowed pursuant to this County travel policy.

3. Travel Advance Settlements

a) Within five (5) working days of completion of travel, the County traveler shall submit all receipts for allowable travel expenses to the Department and within fifteen (15) working days of completion of travel to the Auditor-Controller's Office on a completed County claim form. Credit for the travel advance shall be subtracted from the amount owed to the County traveler.

b) In the event that allowable expenses are less than the amount of the travel advance, the County traveler shall submit the difference in the form of a check or money order made out to the "County of Monterey" with the claim form.

c) County travelers who cannot provide a required receipt shall reimburse the County for the amount of the money advanced to them for that expense.

d) Travelers who do not submit the required documentation by the time frames set forth above may lose their eligibility for future travel advances.

e) Department heads are responsible for ensuring that their employees settle their travel advance claims within the time frames set forth in subsection a) above. Non-compliance may jeopardize advances for the entire department.

B. Prepaid Vendor Claims

1. Vendor Claim Requests

a) Once travel has been authorized, claims to the vendor may be submitted for lodging and registration fees when there is sufficient time for the check to be processed before the authorized County traveler commences travel.

b) If the travel requires a "County of Monterey Travel Request" form, the approved form shall be submitted with the claim. If the original has been submitted with a previous claim, then that shall be noted on the claim form and a copy of the form attached.

c) Whenever possible, the County shall be named as registrant for events to allow

transfer of attendance privilege when conflicts prevent the original registrant from attending.

d) The County will mail the warrant directly to the vendor unless the traveler requests that the warrant be returned to them to hand carry to the vendor.

2. Vendor Claim Settlements

a) Each vendor claim must have an original receipt attached in order to settle the claim. The required receipts for vendor claims that have been prepaid shall be forwarded to the Auditor-Controller's Office within thirty (30) calendar days after completion of travel.

b) Claims paid directly to vendors that are not substantiated by receipts within thirty (30) calendar days of the completion of travel shall be considered to be unsettled travel advances to the County traveler.

c) Department heads are responsible for ensuring that their employees return their receipts within the time frames established by this policy. Non-compliance may jeopardize the department's ability to have travel expenses paid in advance.

d) In the event that all or a portion of the prepaid cost to a vendor is reduced after the check has been processed, the County traveler is responsible for ensuring that the entire difference is returned to the County within the time frames established for settling the claim.

C. Travel Reimbursement Claims

1. After completion of travel, the County traveler shall submit a completed County claim form to the department head for authorization. After review and authorization, the department head shall submit the authorized claim, together with any required receipts, to the Auditor-Controller's Office. Said claim shall be received by the Auditor-Controller's Office within thirty (30) calendar days of the completion of travel.

2. The traveler shall not be reimbursed until s/he has signed the certification for the claim that is required by the Auditor-Controller's Office.

3. The Auditor-Controller's Office shall review the claim for compliance with applicable County policies and procedures. If approved by the Auditor-Controller's Office, the claim shall be processed and a check sent to the claimant within ten (10) working days. If denied, or denied in part, the department's contact person will be notified immediately. The Auditor-Controller has the final decision on allowable expenses.

4. No reimbursement for travel shall be paid to the employee until all required receipts

for the travel claim have been filed with the Auditor-Controller's Office.

5. Travel reimbursements are to be paid via checks and not to be paid via petty cash.

D. Mileage Claims

1. Whenever travel requires advance authorization of the department head, or his/her designee, the resulting mileage expense shall be claimed on the same claim form as the other expenses that apply to that travel. The only exception is if mileage is the only expense of the trip, in which case the traveler may claim the mileage on the monthly "Mileage Reimbursement" claim form.

2. Whenever travel does not require advance authorization of the department head, or his/her designee, the resulting mileage expense shall be claimed on the "Mileage Reimbursement" claim form.

3. Mileage claims shall be submitted monthly, unless the total for the month is less than $50.00, in which case the claim may be held for an additional month. However, the claim must not be held over to the next month more than twice, regardless of the dollar amount.

4. All mileage claims for the last month of the fiscal year must be processed by year-end close.

5. Mileage Claims are to be paid via warrants and not to be paid via petty cash.

E. Reimbursement by Outside Source

1. County travelers receiving reimbursement from an outside source for travel on County time shall forward said reimbursement to the Auditor-Controller for handling and deposit if the traveler intends to submit an expense claim to the County or use County resources, including a County vehicle, to travel. In such cases, the traveler shall then be entitled to submit a claim for actual and necessary expenses for transportation, meals, lodging, and incidentals, subject to the claiming conditions set forth in this travel policy. Said reimbursement shall be delivered to the Auditor-Controller's Office within thirty (30) days of the receipt of the funds.

2. If a County volunteer or non-employee will be receiving a per diem or other reimbursement of travel expenses from a source outside of the County, the volunteer shall not be eligible to claim or receive any additional reimbursement from the County for the same expenses.

F. Late Claims

If a claim for reimbursement or settlement of a travel claim is submitted after the allowed time frames, the payment to the employee shall not be made until the claim has

been reviewed and approved by the Auditor-Controller or his/her designee.

G. Travel Card Use

Subject to the rules contained in the Travel Card Policy, travel expenses (airline, hotel, vehicle rental, gas, emergency repair of county vehicles and airport parking) may be charged to County of Monterey Travel Cards. Prohibited items include employee meals, room service, movies, cash advances, gift cards of any kind, liquor, tobacco and other items prohibited by the Travel Card Policy. Under no circumstances should personal items (even if reimbursed to the county) be charged to the travel card. Expenses paid on the travel card should not be included on a claim for reimbursement.

VII. INTERPRETATIONS

The Auditor-Controller, or his/her designee, shall be responsible for interpretations of this policy.

VIII. EXCEPTIONS

Exceptions to this policy require the approval of the Auditor-Controller or his/her designee.

IX. CONFLICT WITH RULES

In the event that this County Travel policy is in conflict with another County policy, the policy with the strictest application shall prevail.

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("BAA") effective January 1, 2021 ("Effective Date"), is entered into by and among between the County of Monterey, a political subdivision of the State of California, on behalf of Natividad Medical Center ("Covered Entity") and tw-Security, LLC ("Business Associate") (each a "Party" and collectively the "Parties").

RECITALS

A. WHEREAS, Business Associate provides certain Services for Covered Entity that involve the Use and Disclosure of Protected Health Information ("PHI") that is created, received, transmitted, or maintained by Business Associate for or on behalf of Covered Entity.

B. WHEREAS, The Parties are committed to complying with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), and their implementing regulations, including the Standards for the Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subparts A and E (the "Privacy Rule"), the Breach Notification Standards, 45 C.F.R. Part 160 and 164 subparts A and D (the "Breach Notification Rule"), and the Security Standards, 45 C.F.R. Part 160 and Part 164, Subpart C (the "Security Rule"), (collectively "HIPAA"), all as amended from time to time.

C. WHEREAS, The Parties are also committed to complying with the California Confidentiality Laws (defined below).

D. WHEREAS, To the extent that Business Associate is performing activities in connection with covered accounts for or on behalf of Covered Entity, 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").

E. WHEREAS, The Privacy and Security Rules require Covered Entity and Business Associate to enter into a business associate agreement that meets certain requirements with respect to the Use and Disclosure of PHI. This BAA, sets forth the terms and conditions pursuant to which PHI, and, when applicable, Electronic Protected Health Information ("EPHI") shall be handled, in accordance with such requirement.

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

AGREEMENT

1. DEFINITIONS

TW

1.1 All capitalized terms used in this BAA but not otherwise defined shall have the meaning set forth in the Privacy Rule, the Breach Notification Rule, or the Security Rule.

(a) "Breach" shall have the same meaning as "breach" as defined in 45 C.F.R. § 164.402 and shall mean the access, acquisition, Use, or Disclosure of PHI in a manner not permitted under the Privacy Rule that compromises the privacy or security of the PHI; the term "Breach" as used in this BAA shall also mean the unlawful or unauthorized access to, Use or Disclosure of a patient's "medical information" as defined under Cal. Civil Code § 56.05(j), for which notification is required pursuant to Cal. Health & Safety Code 1280.15, or a "breach of the security of the system" under Cal. Civil Code §1798.29.

(b) "California Confidentiality Laws" shall mean the applicable laws of the State of California governing the confidentiality of PHI or Personal Information, including, but not limited to, the California Confidentiality of Medical Information Act (Cal. Civil Code §56, et seq.), the patient access law (Cal. Health & Safety Code §123100 et seq.), the HIV test result confidentiality law (Cal. Health & Safety Code §120975, et seq.), the Lanterman-Petris-Short Act (Cal. Welf. & Inst. Code §5328, et seq.), and the medical identity theft law (Cal. Civil Code 1798.29).

(c) "Protected Health Information" or "PHI" shall mean any information, whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual or the past, present or future payment for the provision of health care to an individual; (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information that can be used to identify the individuals, and (iii) is provided by Covered Entity to Business Associate or created, maintained, received, or transmitted by Business Associate on Covered Entity's behalf. **PHI includes EPHI**.

(d) "Services" shall mean the services for or functions on behalf of Covered Entity performed by Business Associate pursuant to a Services Agreement between Covered Entity and Business Associate to which this BAA applies.

2. PERMITTED USES AND DISCLOSURES OF PHI

Unless otherwise limited herein, Business Associate may:

(a) Use or Disclose PHI to perform Services for, or on behalf of, Covered Entity, provided that such Use or Disclosure would not violate the Privacy or Security Rules, this BAA, or California Confidentiality Laws;

(b) Use or Disclose PHI for the purposes authorized by this BAA or as otherwise Required by Law;

(c) Use PHI to provide Data Aggregation Services for the Health Care Operations of Covered Entity, if required by the Services Agreement and as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B);

TW

(d) Use PHI if necessary for the 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 PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate as 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 person to whom the information is Disclosed that it will remain confidential and be Used or further Disclosed only as Required by Law or for the purpose for which it was Disclosed to the person, and that such person will notify the Business Associate of any instances of which such person is aware that 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); and

(g) De-identify any PHI obtained by Business Associate under this BAA in accordance with 45 C.F.R. § 164.514 and Use or Disclose such de-identified information only as required to provide Services pursuant to the a Services Agreement between the Parties, or with the prior written approval of Covered Entity.

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) Notify the Privacy Officer of Covered Entity, in writing, of: (i) any Use and/or Disclosure of the PHI that is not permitted or required by this BAA; (ii) any Security Incident of which Business Associate becomes aware; and (iii) any suspected Breach. Such notice shall be provided within five (5) business days of Business Associate's discovery of such unauthorized access, acquisition, Use and/or Disclosure. Notwithstanding the foregoing, the Parties acknowledge the ongoing existence and occurrence of attempted but ineffective Security Incidents that are trivial in nature, such as pings and other broadcast service attacks, and unsuccessful log-in attempts. The Parties acknowledge and agree that this Section 3.1(a) constitutes notice by Business Associate to Covered Entity of such ineffective Security Incidents and no additional notification to Covered Entity of such ineffective Security Incidents is required, provided that no such Security Incident results in a Breach. A ransomware attack shall not be considered an ineffective Security Incident and shall be reported to Covered Entity, irrespective of whether such Security Incident results in a Breach. Business Associate shall investigate each Security Incident or unauthorized access, acquisition, Use, or Disclosure of PHI, or suspected Breach that it discovers and shall provide a summary of its investigation to Covered Entity, upon request. If Business Associate or Covered Entity determines that such Security Incident or unauthorized access, acquisition, Use, or Disclosure, or suspected Breach constitutes a Breach, then Business Associate shall comply with the requirements of Section 3.1(a)(i) below;

TW

(i) Business Associate shall provide a supplemental written report in accordance with 45 C.F.R. § 164.410(c), which shall include, to the extent possible, the identification of each individual whose PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, Used or Disclosed during the Breach, to Covered Entity without unreasonable delay, but no later than five (5) business days after discovery of the Breach;

(ii) Covered Entity shall have sole control over the timing and method of providing notification of such Breach to the affected individual(s), the appropriate government agencies, and, if applicable, the media. Business Associate shall assist with the implementation of any decisions by Covered Entity to notify individuals or potentially impacted individuals;

(b) In consultation with the Covered Entity, Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to the Business Associate of such improper access, acquisition, Use, or Disclosure, Security Incident, or Breach. Business Associate shall take prompt corrective action, including any action required by applicable State or federal laws and regulations relating to such Security Incident or non-permitted access, acquisition, Use, or Disclosure. Business Associate shall reimburse Covered Entity for its reasonable costs and expenses in providing any required notification to affected individuals, appropriate government agencies, and, if necessary the media, including, but not limited to, any administrative costs associated with providing notice, printing and mailing costs, public relations costs, attorney fees, and costs of mitigating the harm (which may include the costs of obtaining up to one year of credit monitoring services and identity theft insurance) for affected individuals whose PHI or Personal Information has or may have been compromised as a result of the Breach;

(c) Implement appropriate administrative, physical, and technical safeguards and comply with the Security Rule to prevent Use and/or Disclosure of EPHI other than as provided for by this BAA;

(d) Obtain and maintain a written agreement with each of its Subcontractors that creates, maintains, receives, Uses, transmits or has access to PHI that requires such Subcontractors to adhere to the substantially the same restrictions and conditions with respect to PHI that apply to Business Associate pursuant to this BAA;

(e) Make available all internal practices, records, books, agreements, policies and procedures and PHI relating to the Use and/or Disclosure of PHI received from, created, maintained, or transmitted by Business Associate on behalf of Covered Entity to the Secretary of the Department of Health and Human Services ("Secretary") in a time and manner designated by the Secretary for purposes of determining Covered Entity's or Business Associate's compliance with the Privacy Rule. In addition, Business Associate shall promptly make available to Covered Entity such books, records, or other information relating to the Use and Disclosure of PHI for purposes of determining whether Business Associate has complied with this BAA or maintains adequate security safeguards, upon reasonable request by Covered Entity;

TW

(f) Document Disclosures of PHI and information related to such Disclosure and, within thirty (30) 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. 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 ten (10) 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 thirty (30) days of the termination of this BAA, the PHI in its possession and retain no copies, including backup copies;

(h) Disclose to its Subcontractors 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 to Covered Entity to meet a request by an individual under 45 C.F.R. § 164.524. Business Associate shall notify Covered Entity within ten (10) days of its receipt of a request for access to PHI from an Individual; 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. Business Associate shall notify Covered Entity within ten (10) days of its receipt of a request for amendment of PHI from an Individual;

(j) If applicable, 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) To the extent that Business Associate carries out one or more of Covered Entity's obligations under the Privacy Rule, Business Associate shall comply with the requirements of the Privacy Rule that apply to Covered Entity in the performance of such obligations;

(l) Unless prohibited by law, 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; and

(m) Maintain policies and procedures materially in accordance with State Confidentiality 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.

3.2 Business Associate Acknowledgment.

(a) 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.

(b) Business Associate further acknowledges that it is obligated by law to comply, and represents and warrants that it shall comply, with HIPAA and the HITECH Act. Business Associate shall comply with all California Confidentiality Laws, to the extent that such state laws are not preempted by HIPAA or the HITECH Act.

(c) Business Associate further acknowledges that uses and disclosures of protected health information must be consistent with NMC's privacy practices, as stated in NMC's Notice of Privacy Practices. The current Notice of Privacy Practices can be retrieved online at: http://www.natividad.com/quality-and-safety/patient-privacy . ← broken link TW Business Associate agrees to review the NMC Notice of Privacy Practices at this URL at least once annually while doing business with NMC to ensure it remains updated on any changes to the Notice of Privacy Practices NMC may make.

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 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;

(c) 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

(d) Notify Business Associate 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. TERM AND TERMINATION

4.1 **Term**. This BAA shall become effective on the Effective Date and shall continue in effect unless terminated as provided in this Section 4. Certain provisions and requirements of this BAA shall survive its expiration or other termination as set forth in Section 5 herein.

4.2 **Termination**. If Covered Entity determines in good faith that Business Associate has breached a material term of this BAA, Covered Entity may either: (i) immediately terminate this BAA and any underlying Services Agreement; or (ii) terminate this BAA and any underlying Services Agreement within thirty (30) days of Business Associate's receipt of written notice of such breach, if the breach is not cured to the satisfaction of Covered Entity.

4.3 **Automatic Termination**. This BAA 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 BAA for any reason, Business Associate shall return all PHI pursuant to 45 C.F.R. § 164.504(e)(2)(ii)(J) if, and to the extent that, it is feasible to do so. Prior to returning the PHI, Business Associate shall recover any PHI in the possession of its Subcontractors. 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 with 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. In such event, Business Associate shall: (i) retain only that PHI which is necessary for Business Associate to continue its proper management and administration or carry out its legal responsibilities; (ii) return to Covered Entity the remaining PHI that the Business Associate maintains in any form; (iii) continue to extend the protections of this BAA to the PHI for as long as Business Associate retains PHI; (iv) limit further Uses and Disclosures of such PHI to those purposes that make the return or destruction of the PHI not feasible and subject to the same conditions as set out in Section 2 above, which applied prior to termination; and (vi) return to Covered Entity the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

5. MISCELLANEOUS

5.1 **Survival**. The respective rights and obligations of Business Associate and Covered Entity under the provisions of Sections 2.1, 4.4, 5.7, 5.8, 5.11, and 5.12 shall survive termination of this BAA until such time as the PHI is returned to Covered Entity or destroyed. In addition, Section 3.1(i) shall survive termination of this BAA, 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 BAA 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 HIPAA, the HITECH Act, or California Confidentiality

Laws is materially amended in a manner that changes the obligations of the Parties, the Parties agree to negotiate in good faith appropriate amendment(s) to this BAA to give effect to the revised obligations. Further, no provision of this BAA 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 BAA 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:

TW-SECURITY, LLC
Attn: TOM WALSH
6108 W 121ST STREET
OVERLAND PARK, KS 66209
Phone: 913-696-1573
~~Fax:~~ EMAIL TOM.WALSH@TW-SECURITY.COM

If to Covered Entity, to:
Natividad Medical Center
Attn: Compliance/Privacy Officer
1441 Constitution Blvd.
Salinas, CA 93906
Phone: 831-755-4111
Fax: 831-755-6254

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 BAA 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 Relationship of Parties. Notwithstanding anything to the contrary in the Services Agreement, Business Associate is an independent contractor and not an agent of Covered Entity under this BAA. Business Associate has the sole right and obligation to supervise, manage, contract, direct, procure, perform, or cause to be performed all Business Associate obligations under this BAA.

5.7 Choice of Law; Interpretation. This BAA shall be governed by the laws of the State of California. Any ambiguities in this BAA shall be resolved in a manner that allows Covered Entity and Business Associate to comply with the Privacy Rule, the Security Rule, and the California Confidentiality Laws.

5.8 Indemnification. Business Associate shall indemnify, defend, and hold harmless the County of Monterey (the "County"), its officers, agents, and employees from any claim, liability, loss, injury, cost, expense, penalty or damage, including costs incurred by the County with respect to any investigation, enforcement proceeding, or third party action, arising out of, or in connection with, a violation of this BAA or a Breach that is attributable to an act or omission of Business Associate and/or its agents, members, employees, or Subcontractors, 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 provide the broadest possible indemnification for the County. This provision is in addition to, and independent of, any indemnification provision in any related or other agreement between the Parties.

5.9 Applicability of Terms. This BAA applies to all present and future Service Agreements and Business Associate relationships, written or unwritten, formal or informal, in which Business Associate creates, receives, transmits, or maintains any PHI for or on behalf of Covered Entity in any form whatsoever. This BAA shall automatically be incorporated in all subsequent agreements between Business Associate and Covered Entity involving the Use or Disclosure of PHI whether or not specifically referenced therein. In the event of any conflict or inconsistency between a provision of this BAA and a provision of any other agreement between Business Associate and Covered Entity, the provision of this BAA shall control unless the provision in such other agreement establishes additional rights for Business Associate or additional duties for or restrictions on Business Associate with respect to PHI, in which case the provision of such other agreement will control.

5.10 Insurance. In addition to any general and/or professional liability insurance required of Business Associate, Business Associate agrees to obtain and maintain, at its sole expense, liability insurance on an occurrence basis, covering any and all claims, liabilities, demands, damages, losses, costs and expenses arising from a breach of the obligations of Business Associate, its officers, employees, agents and Subcontractors under this BAA. Such insurance coverage will be maintained for the term of this BAA, and a copy of such policy or a certificate evidencing the policy shall be provided to Covered Entity at Covered Entity's request.

5.11 Legal Actions. Promptly, but no later than five (5) business days after notice thereof, Business Associate shall advise Covered Entity of any actual or potential action, proceeding, regulatory or governmental orders or actions, or any material threat thereof that becomes known to it that may affect the interests of Covered Entity or jeopardize this BAA, and of any facts and circumstances that may be pertinent to the prosecution or defense of any such actual or potential legal action or proceeding, except to the extent prohibited by law.

TW

5.12 **Audit or Investigations**. Promptly, but no later than five (5) calendar days after notice thereof, Business Associate shall advise Covered Entity of any audit, compliant review, or complaint investigation by the Secretary or other state or federal agency related to compliance with HIPAA, the HITECH Act, or the California Confidentiality Laws.

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

BUSINESS ASSOCIATE	**COVERED ENTITY**
By: Thomas R. Walsh	By:
Print Name THOMAS R. WALSH	Print Name: Gary R. Gray
Print Title FOUNDER & MANAGING PARTNER	Print Title: Chief Executive Officer
Date: DECEMBER 1, 2020	Date: 12/11/2020

Note: *The consulting services provided by tw-Security under our Statement of Work (a.k.a. "Exhibit A – Scope of Services" as used in this BAA) would not include creating, receiving, storing/retaining, using, disclosing, and/or transmitting Protected Health Information (PHI) as defined by the definition of a Business Associate in 45 CFR §160.103.*

Any access to PHI during the engagement would be incidental.

TW