

TULARE COUNTY AGREEMENT NO. _____

**COUNTY OF TULARE
HEALTH & HUMAN SERVICES AGENCY
SERVICES AGREEMENT**

THIS AGREEMENT ("Agreement") is entered into as of _____ between the **COUNTY OF TULARE**, a political subdivision of the State of California ("**COUNTY**"), and **Medina & Yeargin, Inc. ("CONTRACTOR")**. **COUNTY** and **CONTRACTOR** are each a "**Party**" and together are the "**Parties**" to this Agreement, which is made with reference to the following:

- A.** **COUNTY** wishes to retain the services of **CONTRACTOR** for the purpose of providing consultation services to ensure **HHSA** meets the governmental demands for cyber security and privacy
- B.** **CONTRACTOR** has the experience and qualifications to provide the services **COUNTY** requires pertaining to the Tulare County Health and Human Services Agency; and
- C.** **CONTRACTOR** is willing to enter into this Agreement with **COUNTY** upon the terms and conditions set forth herein.

THE PARTIES AGREE AS FOLLOWS:

- 1. TERM:** This Agreement becomes effective as of February 1, 2018 and expires at 11:59 PM on December 31, 2018, unless earlier terminated as provided below, or unless the Parties extend the term by a written amendment to this Agreement.
- 2. SERVICES:** See attached Exhibit A.
- 3. PAYMENT FOR SERVICES:** See attached Exhibit B.
- 4. INSURANCE:** Before approval of this Agreement by **COUNTY**, **CONTRACTOR** must file with the Clerk of the Board of Supervisors evidence of the required insurance as set forth in the attached **Exhibit C**.
- 5. GENERAL AGREEMENT TERMS AND CONDITIONS:** **COUNTY'S** "General Agreement Terms and Conditions" are hereby incorporated by reference and made a part of this Agreement as if fully set forth herein. **COUNTY'S** "General Agreement Terms and Conditions" can be viewed at <http://tularecountycounsel.org/default/index.cfm/public-information/>
- 6. ADDITIONAL EXHIBITS:** **CONTRACTOR** shall comply with the terms and conditions of the Exhibits listed below and identified with a checked box, which are by this reference made a part of this Agreement. Complete Exhibits D, E, F, G, G-1, and H can be viewed at <http://tularecountycounsel.org/default/index.cfm/public-information/>

**COUNTY OF TULARE
HEALTH & HUMAN SERVICES AGENCY
SERVICES AGREEMENT**

<input checked="" type="checkbox"/>	Exhibit D	Health Insurance Portability and Accountability Act (HIPAA) Business Associate Agreement
<input checked="" type="checkbox"/>	Exhibit E	Cultural Competence and Diversity
<input checked="" type="checkbox"/>	Exhibit F	Information Confidentiality and Security Requirements
<input type="checkbox"/>	Exhibit G	Contract Provider Disclosures (<u>Must be completed by Contractor and submitted to County prior to approval of agreement.</u>)
<input type="checkbox"/>	Exhibit G1	National Standards for Culturally and Linguistically Appropriate Services (CLAS) in Health and Health Care
<input type="checkbox"/>	Exhibit H	Additional terms and conditions for federally-funded contracts
<input type="checkbox"/>	Exhibit ____	[Insert name of any other exhibit needed and attach]

7. NOTICES: (a) Except as may be otherwise required by law, any notice to be given must be written and must be either personally delivered, sent by facsimile transmission or sent by first class mail, postage prepaid and addressed as follows:

COUNTY:

Contracts Unit
Tulare County Health and Human
Services Agency
5957 S. Mooney Blvd.
Visalia, CA 93277
Phone No.: 559-624-8000
Fax No.: 559-713-3718

With a Copy to:

COUNTY ADMINISTRATIVE OFFICER
2800 W. Burrell Ave.
Visalia, CA 93291
Phone No.: 559-636-5005
Fax No.: 559- 733-6318

CONTRACTOR:

Medina & Yeargin, Inc.
733 Belfast Court
Galt, CA 95632
Phone No.: 209-712-7172

(b) Notice personally delivered is effective when delivered. Notice sent by facsimile transmission is deemed to be received upon successful transmission. Notice sent by first class mail will be deemed received on the fifth calendar day after the date of mailing. Either Party may change the above address by giving written notice under this section.

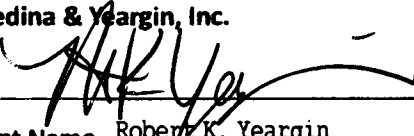
8. AUTHORITY: CONTRACTOR represents and warrants to COUNTY that the individual(s) signing this Agreement on its behalf are duly authorized and have legal capacity to sign this Agreement and bind CONTRACTOR to its terms. CONTRACTOR acknowledges that COUNTY has relied upon this representation and warranty in entering into this Agreement.

**COUNTY OF TULARE
HEALTH & HUMAN SERVICES AGENCY
SERVICES AGREEMENT**

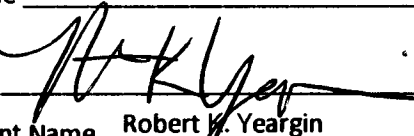
9. COUNTERPARTS: The Parties may sign this Agreement in counterparts, each of which is an original and all of which taken together form one single document.

THE PARTIES, having read and considered the above provisions, indicate their agreement by their authorized signatures below.

Date: November 16, 2018

By 
Print Name Robert K. Yeargin
Title Chairman, Medina & Yeargin, Inc

Date: November 16, 2018

By 
Print Name Robert K. Yeargin
Title President, Medina & Yeargin, Inc

[Pursuant to Corporations Code section 313, County policy requires that contracts with a Corporation be signed by both (1) the chairman of the Board of Directors, the president or any vice-president (or another officer having general, operational responsibilities), and (2) the secretary, any assistant secretary, the chief financial officer, or any assistant treasurer (or another officer having recordkeeping or financial responsibilities), unless the contract is accompanied by a certified copy of a resolution of the corporation's Board of Directors authorizing the execution of the contract. Similarly, pursuant to California Corporations Code section 17703.01, County policy requires that contracts with a Limited Liability Company be signed by at least two managers, unless the contract is accompanied by a certified copy of the articles of organization stating that the LLC is managed by only one manager.]

COUNTY OF TULARE

Date: _____ By _____
Chairman, Board of Supervisors

ATTEST: JASON T. BRITT
County Administrative Officer/Clerk of the Board
of Supervisors of the County of Tulare

By _____
Deputy Clerk

Approved as to Form
County Counsel

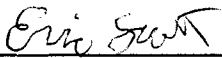
By 
Deputy
Matter # 20181278

Exhibit A

Scope of Work

The scope of work consists of the analysis, assessment and completion of the HIPAA Security and MEDS Risk Assessment; to include: audit, review, and other due diligence activities in order to identify risks, and to implement remediation options to manage those risks. The analysis and assessment will result in addressing identified risks through a remediation plan in preparation for implementation of Tulare County Health & Human Services Agency's (TCHHSA) HIPAA Security Program. This will assist with ensuring TCHHSA's Compliance with State and Federal Privacy and Security Regulations.

A. Information Security Risk Assessment

Evaluate compliance with regulatory requirements, industry standards, and best practices (HIPAA Rules-1996, HITECH Act -2009, HIPAA Rule-2013, NIST SP800-53) and Medi-Cal Eligibility Data System (MEDS) Privacy and Security Agreement (PSA) considering each of the following standards:

45 CFR Part 160,

- Subpart A – General Provisions;
- Subpart B – Preemption of State Law;
- Subpart C – Compliance and Investigation;
- Subpart D – Imposition of Civil Money Penalties;
- Subpart E – Procedures for Hearings
- 164.306 General Requirements

45 CFR Part 164, Subpart C – Security Standards for the Protection of Electronic Protected Health Information (ePHI)

- 164.308 Administrative Safeguards
- 164.310 Physical Safeguards
- 164.312 Technical Safeguards
- 164.316 Policies, Procedures, and Documentation

Medi-Cal Eligibility Data System (MEDS) PSA Review

Identify information assets (systems, data, and information processing facilities) that contain, store, maintain, support, and transmit electronic protected health information (ePHI).

Identify potential risk(s) to the confidentiality, integrity, and availability of ePHI:

- Evaluate the methods by which departments and divisions collect, use, manage, store, maintain, disclose, and dispose of ePHI.
- Assess the design and effectiveness of existing security measures.

Evaluate Compliance with the NIST Security Control Standards (NIST SP800-53).

Compare the HIPAA Privacy and Security Rule Requirements with those of applicable California State Privacy, Security and Confidentiality Statutes:

- Identify state statutes that are more restrictive than the HIPAA Regulation; and
- Determine the extent to which the most stringent requirements are met.

Consider current security controls, policies, standards, and contractual requirements:

- Conduct physical surveys of all departmental sites and facilities that are in scope, and determine if building or space modifications are required for compliance.
- Evaluate HIPAA breach incident reporting and response procedures
- Review contracts and agreements (including Joint Powers Agreements, Memoranda of Understanding, Government Service Agreements, and Business Associate Agreements) for HIPAA compliance.
- Review HIPAA-related agreements for new employees, independent contractors, and volunteers.
- Compare current security practices, including: data management, disposal and encryption, and ePHI handling and monitoring practices with current HIPAA requirements.

Recommend realistic controls and remediation activities to enhance the security posture, and improve compliance with: HIPAA Security Rules, the HITECH Act, and the NIST standards:

- Develop a priority list of security measures and remediation activities for implementation.
- Suggest one or more options (i.e. policies, procedures, technical controls, and/or technologies) for each identified risk:
 - Include estimated cost, and level of effort required to implement each option; and
 - Map each security measure to the appropriate regulatory standard.
- For “Addressable” HIPAA implementation specifications that are unreasonable or inappropriate, document alternative security measures:
 - Document alternative measures that have already been implemented;
 - Document how the alternative measures satisfy HIPAA standards; and,
 - Document the reason why the HIPAA implementation specification is unreasonable or inappropriate, and how the security measures satisfy the higher-level HIPAA standard.

B. Technical Risk Assessment

Identify and evaluate Technical Information Security Risk, and provide actionable solutions to enhance the security of electronic personally identifiable information (ePII), ePHI, and other sensitive information assets.

Methodology: Provide TCHHSA with a HIPAA/HITECH security focused network architecture review. This review will highlight current strengths and weaknesses of implemented controls, and the business drivers for those controls that remediate access and services to and from IT infrastructure. Using a variety of network and device scanning tools in cooperation with TCiCT employees, perform at least two scans of TCiCT network supporting HIPAA/HITECH systems. Systems identified in the process that do not assist in the support of HIPAA/HITECH compliance would be eliminated from the assessment, and would not be reported. References (including related references) to conduct assessment include: NIST SP800 series standards, California SAM Chapter 5300 Information Security (Sept 2013) and Statewide Health Information Policy Manual (SHIPM).

Privacy Consulting Group uses Kali Linux Tools, NESSUS, Qualsys, Nipper, and other proprietary tools to conduct intelligence gathering in support of TCiCT Information Security Risk Assessment protocol. The selected tools for use in this project will be approved and coordinated with TCiCT and TCHHSA. No covert or overt events will proceed without permission.

These technical risk assessments shall include:

Network Security Assessment-Provides a security-focused network architecture review, highlighting current strengths and weaknesses of implemented controls and the business drivers for those controls that remediate access and services to and from the IT infrastructure. The Technical Security Assessment Review Report will include:

- Network Topology
- Network Switch(es) Configuration
- Endpoint Access
- Firewall(s) Configuration
- IDP/IDS Configuration
- Router Configuration
- Virtual Private Network (VPN) Configuration
- WLAN Configuration
- Other Network based security controls (e.g. Content Filtering, Antispam, etc.)

Host / Server Security Assessment - working in cooperation and with each department (as necessary) will conduct Host Server Security Assessment using scanning tools and physical onsite analyses to review and document findings for each department. Host Server Assessment (Hardening) will include:

- Server Security Planning;

- Securing Server OS;
- Securing Server Software;
- Maintaining Security of Server;
- Host Server Assessment (OS and 3rd party software); and
- Host Server Assessment (Host Dependencies at Service/End User point)

Endpoint Security Assessment—working in cooperation and with each department (as necessary) will conduct an assessment of the following Endpoint Security areas:

- **Workstation Configuration**
Select and identify workstations and laptops for configuration review.
- **Endpoint encryption**
Review and confirm type of endpoint encryption in place.
- **User Rights (Local/Domain)**
Review and analyze local and domain group policies and management for authorized access and restrictions of users in department.
- **Media Access**
Determine standard policy and procedure for use of mobile/portable media devices, and required security measures when used for ePHI and ePIL. Review and document physical media access controls (placement of screens, printers, copiers, paper files, file cabinets, paper file storage (archived file rooms)) and methods used to prevent unauthorized visitors from access to ePHI/PHI.
- **Password Practices**
Review each department's password practices and determine whether strong passwords are incorporated into user accounts, and minimum standards by Federal and State authority are observed.
- **OS and Third-Party Software Patching**
Review and analyze TCICT/Department software patching management program. Document the OS version and third-party software for latest updates. Review patch logs for accuracy, install history, documentation, management authorization, and administrator sign-off.
- **Peripheral Devices (network printers, scanners) configuration**
Identify, review, and analyze all peripheral devices supporting HIPAA/HITECH/Omnibus operations for security configuration, access, logs, hard drive encryption, and support agreements regarding disposal of internal memory and device storage capabilities. Recommend best practice for physical access and place of devices, user access, and passwords/PIN configuration

Application Security Assessment

- Conduct an application security assessment that analyzes the Internet, Extranet, and Intranet applications for existence and strength of application security controls. Assessment will be conducted in accordance with the OWASP reference and other baselines for application security (e.g. assessment of authentication mechanisms and authorization mechanisms, session context control mechanisms, audit logging, intrusion detection and deterrence).

- Conduct an Application Security Assessment that targets the security capabilities of critical applications. Assess whether the applications have capabilities to secure information/data communications, and whether the capabilities have been fully utilized.
- For in-house developed applications, the overall security framework used for the application development process will be reviewed.
- The application security review will evaluate available security features, and security-relevant configuration items within the application, to conclude whether those controls have been configured to provide the level of protection required by business, regulatory and corporate drivers.

C. Non-Technical Risk Assessment

Review of HIPAA Security training and other security awareness efforts to determine whether gaps exist between training content and HIPAA Privacy and Security standards, state privacy and security statutes, and general level of information security awareness among different levels of staff including the efficiency of training initiatives.

The assessment is performed by conducting surveys of selected users to determine user's awareness, their basic security responsibilities, people to contact if they have questions and where to obtain current Privacy and Security policies and procedures. This assessment includes:

End User Security Awareness Assessment

- Evaluate the effectiveness of security training program:
 - Interview personnel responsible for security training;
 - Review policies regarding staff training and user security awareness;
 - Review security awareness presentations and other training materials;
 - Work with assigned staff to develop and conduct staff surveys based on policies and security awareness presentations;
 - Distribute surveys to a random sample of employees; and,
 - Analyze survey results to determine the staff's overall understanding of the topics presented in educational materials and training sessions.
- Perform social engineering:
 - Perform email phishing, phone pre-texting, baiting and/or tailgating techniques; and,
 - Determine the value of information obtained.
- Recommend improvements to the security training program, and other security awareness training:
 - Identify gaps between training content and regulatory standards (HIPAA Security Rules and California privacy and security statutes); and,
 - Develop a priority list of topics that should be addressed within training program(s).

Physical Security Assessment

- Evaluate the design and effectiveness of physical security controls in place at facilities where PHI and ePHI are stored, maintained, received, and transmitted.
- Develop a priority list of security measures and remediation activities for implementation.

D. Deliverables

Following is a list of all project deliverables:

Deliverable	Description
Complete and Finalize Security Risk Assessment	Executive Summary - Introduction and scope, Approach and methodology, Findings (with associated risk ranking), actionable recommendations and remediation plan; and Technician's Notes
Conduct annual review of TCHHSA Security Risk Assessment	PCG will review, document, and update changes and progress of recommended remediation plan noted in risk analysis. Provide an updated gap analysis and monitor ongoing efforts

E. Timeline for Execution

Key project dates are outlined below. Dates are best-guess estimates and are subject to change until a contract is executed.

Description	Start Date	End Date
Complete and Finalize Security Risk Assessment and Analysis	2/1/2018	12/31/2018
Project End	2/1/2018	12/31/2018

F. Supplied Material

The following materials are to be supplied by TCHSSA on this project in order for Privacy Consulting Group to meet project milestones. This material must be supplied on schedule. The due dates included in the following table represent our best guess based on current proposed project dates:

Materials to be supplied by TCHSSA	Due Date*
Workspace and/or small conference meeting area with onsite access to County Network, internet.	12/31/2018
Virtual Private Network access to TCHHSA County network, and access to secure network storage shared drive	12/31/2018

EXHIBIT B

G. Pricing

The following table details the pricing for delivery of the services outlined in this proposal. This pricing is valid for 60 days from the date of this proposal:

Services Cost	Price
Consulting Services	
400 consulting hours (min) @ \$75 per hour	\$30,000

Preferred pricing is at a reduced flat rate for Tulare County as a repeat customer and extended length of contract. Total pricing includes all expenses incurred by Privacy Consulting Group for work completed on site.

**Disclaimer: The prices listed in the preceding table are an estimate for the services discussed. This summary is not a warranty of final price. Estimates are subject to change if project specifications are changed, or costs for outsourced services change before a contract is executed. Purchase and implementation of additional software and/or support services, not included.*

**We cannot be responsible for cost overruns caused by client's failure to deliver materials by agreed-upon due dates.*

EXHIBIT C

NON-PROFESSIONAL SERVICES **INSURANCE REQUIREMENTS**

CONTRACTOR shall provide and maintain insurance for the duration of this Agreement against claims for injuries to persons and damage to property which may arise from, or in connection with, performance under the Agreement by the CONTRACTOR, his agents, representatives, employees and subcontractors, if applicable.

A. Minimum Scope & Limits of Insurance

1. Commercial General Liability coverage of \$1,000,000 on an occurrence basis, including products and completed operations, property damage, bodily injury and personal & advertising injury (occurrence Form CG 00 01). If a general aggregate applies, either the general aggregate limit shall apply separately to this project/location (ISO CG 25 03 or 25 04) or the general aggregate limit must be no less than \$2,000,000.
2. Insurance Services Office Form Number CA 00 01 covering Automobile Liability, (any auto) of no less than \$1,000,000 per accident for bodily injury and property damage. If an annual aggregate applies it must be no less than 2,000,000.
3. Workers' Compensation insurance as required by the State of California, with Statutory Limits, and Employer's Liability Insurance with limit of no less than \$1,000,000 per accident for bodily injury or disease.

B. Specific Provisions of the Certificate

1. If any of the required insurance is written on a claims made form, the retroactive date must be before the date of the contract or the beginning of the contract work and must be maintained and evidence of insurance must be provided for at least three (3) years after completion of the contract work.
2. CONTRACTOR must submit endorsements to the General Liability reflecting the following provisions:
 - a. *The COUNTY OF TULARE, its officers, agents, officials, employees and volunteers are to be covered as additional insureds as respects: liability arising out of work or operations performed by or on behalf of the Contractor including materials, parts, or equipment furnished in connection with such work or operation.*
 - b. *For any claims related to this project, the CONTRACTOR's insurance coverage shall be primary insurance at least as broad as ISO CG 20 01 01 13 as respects the COUNTY, its officers, agents, officials, employees and volunteers. Any insurance or self-insurance maintained by the COUNTY, its officers, agents, officials, employees or volunteers shall be excess of the CONTRACTOR's insurance and shall not contribute with it.*
 - c. *Each insurance policy required by this agreement shall provide that coverage shall not be canceled, except with written notice to the COUNTY.*
 - d. *CONTRACTOR hereby grants to COUNTY a waiver of any right to subrogation which any insurer of the CONTRACTOR may acquire against the COUNTY by virtue of the payment of any loss under such insurance. CONTRACTOR agrees to obtain any endorsement that may be necessary to affect this waiver of subrogation, but this provision applies regardless of whether or not the COUNTY has received a waiver of subrogation endorsement from the insurer.*

3. The Workers' Compensation policy shall be endorsed with a waiver of subrogation in favor of the COUNTY for all work performed by the CONTRACTOR, its employees, agents and subcontractors. CONTRACTOR waives all rights against the COUNTY and its officers, agents, officials, employees and volunteers for recovery of damages to the extent these damages are covered by the workers compensation and employers liability.

C. Deductibles and Self-Insured Retentions

Deductibles and self-insured retentions must be declared and any deductible or self-insured retention that exceeds \$100,000 will be forwarded to the COUNTY Risk Manager for approval.

D. Acceptability of Insurance

Insurance must be placed with insurers with a current rating given by A.M. Best and Company of no less than A-:VII and a Standard & Poor's rating (if rated) of at least BBB and from a company approved by the Department of Insurance to conduct business in California. Any waiver of these standards is subject to approval by the County Risk Manager.

E. Verification of Coverage

Prior to approval of this Agreement by the COUNTY, the CONTRACTOR shall file with the submitting department, certificates of insurance with original endorsements effecting coverage in a form acceptable to the COUNTY. Endorsements must be signed by persons authorized to bind coverage on behalf of the insurer. The COUNTY reserves the right to require certified copies of all required insurance policies at any time.