AMENDMENT TO ORDER OF COMMISSIONERS COURT
Authorizing the expenditure of funds

The Commissioners Court of Harris County, Texas, convened at a meeting of said Court at the Harris County Administration Building in the City of Houston, Texas, on the ____ day of _____, 2024 with all members present except _____.

A quorum was present. Among other business, the following was transacted:

AMENDEDMENT TO ORDER UNDER JOB NO. 21-0317 WITH ERNST & YOUNG LLP TO UPDATE THE STATEMENT OF WORK AT NO COST

THE ORDER AUTHORIZING THE EXPENDITURE OF FUNDS FOR CONSULTING SERVICES UNDER JOB 21-0317 WITH ERNST & YOUNG LLP WAS APPROVED AT COMMISSIONERS COURT ON JUNE 27, 2023, ITEM 23-3539

THE AGREEMENT WITH ERNST & YOUNG LLP WAS APPROVED AT COMMISSIONERS COURT ON MARCH 22, 2022, ITEM 22-2097

Commissioner _____ introduced an Order and made a motion that the same be adopted. Commissioner _____ seconded the motion for adoption of the Order. The motion, carrying with it the adoption of the Order, prevailed by the following vote:

Vote of the Court	Yes	No	Abstain
Judge Hidalgo	□	□	□
Comm. Ellis	□	□	□
Comm. Garcia	□	□	□
Comm. Ramsey, P.E.	□	□	□
Comm. Briones	□	□	□

The County Judge thereupon announced that the motion had duly and lawfully carried and that the Order had been duly and lawfully adopted. The Order thus adopted follows:

IT IS ORDERED the Harris County Judge is authorized to approve for and on behalf of Harris County the expenditure of $1,867,500.00 in funds under Job No. 21-0317 for the Agreement between Harris County and Ernst & Young LLP. The expenditure will provide business and technology consulting services for the establishment of a new compliance office ("Services"). The amended "Proposal to Serve: Harris County Risk & Compliance Assessment and Enablement" and the Agreement are incorporated herein as though fully set forth word-for-word.

The Services provided under this Order will meet 10% MWBE participation through the use of MPACT Strategic Consulting LLC.

All Harris County officials and employees are authorized to do any and all things necessary or convenient to accomplish the purpose of this Order.

STATEMENT OF WORK
SUBMITTED BY
ERNST & YOUNG LLP

Background
Harris County Public Health (HCPH) is the health department for Harris County that provides comprehensive health services and programs to the community through a workforce of approximately 700 public health professionals – all dedicated to improving the health and well-being of Harris County residents and the communities in which they live, learn, work, worship, and play. The HCPH jurisdiction included approximately 2.5 million people and over 30 other municipalities located in Harris County (not including the city of Houston).

HCPH is seeking to establish an office of Public Health and Healthcare compliance with the necessary surrounding infrastructure and operating model. The primary outcomes of this include eliminating fraud, waste and abuse; institutionalizing the appropriate policies and standards; protecting health data and other critical data; and deploying an effective compliance monitoring plan.

Objective
The objective is to (1) provide the HCPH with a public health compliance program design based on the United States Department of Health and Human Services (DHHS) Office of Inspector General (OIG) 7 Elements of a Compliance Program, (2) a strategic roadmap to implement the proposed compliance program, (3) provide a health privacy and security assessment, and (4) baseline health/public health compliance risk assessment. HCPH's endeavors to establish a program in order to proactively prevent, detect, respond to, and report violations of laws, government regulations and ethical rules.

1. Scope

1.1. Services

Vendor shall provide business and technology consulting services in support of Public Health's assessment, planning, and execution of a Compliance function. Vendor shall run four (4) workstreams through twelve (12) months period of performance:

1.1.1. Health/Public Health Compliance Program Development

This scope area shall focus on developing a Health/Public Health Compliance program that includes The United States Department of Health & Human Services Office of Inspector General (OIG) seven elements of a compliance program to prevent fraud, waste, and abuse as well as to maintain internal controls to monitor adherence to applicable statutes, regulations and federal program requirements.

- Governance Structure and Compliance Committee (RFO Requirements A.2) - Develop governance structure and suggestions for the composition of the Compliance Committee and frequency and content of updates and discussions
- Communication Plan (RFO Requirements A.4) - Develop a communication plan that clearly identifies stakeholders and the channels of communication
- Policies and Procedures (RFO Requirements A.1) - Informed by the risk assessment and roadmap, work with the compliance office to draft policies and procedures for the

office and provide recommendations and support as needed to program offices where updates to policies and procedures or new policies and procedures are required

- Review standards of conduct and disciplinary guidelines (RFO Requirements A.1, A.6, A.7) - Review and provide comments and recommendations to existing standards of conduct and disciplinary guidelines
- Draft Training Plan (RFO Requirements A.3) - Understand the compliance requirements and develop training plan the ensures all employees obtain the required training timely
- Procedures for conducting audits and monitoring (RFO Requirements A.5) - Develop processes and procedures to support the conducting of ongoing internal monitoring and auditing. Items to be developed include metrics, audit planning process, testing procedures, report guidelines, recommendation tracking, etc.
- Remediation plans and corrective action tracking (RFO Requirements A.5, A.7) - Develop procedures to log, report, track and confirm actions taken for instances of noncompliance

1.1.2. Health/Public Health Compliance Risk Assessment

Vendor shall assist in completing the assessment of the current infrastructure and compliance readiness. Specific activities shall include:

- Compliance Catalogue (RFO Requirements B.1) - Catalogue of relevant federal, state and local healthcare and public health requirements.
- Regulatory Requirements mapped to Organizational Structure (RFO Requirements B.2) - Current HCPH organizational structure, including governing body, departments, programs, offices and divisions and map of key functional areas for which compliance oversight and regulations are applicable.
- Gap analysis (RFO Requirements B.3)- Document detailing any gaps identified in the HCPH compliance landscape, including insufficient or nonexistent compliance policies and procedures associated with relevant local, state, and federal regulations and the OIG's 7 elements on compliance.
- Risk assessment (RFO Requirements B.4, C.1) - Document detailing any risks resulting from the identified gaps, the regulations and policies associated with those risks, and their impact to HCPH's compliance posture.

1.1.3.Health/Public Health Compliance Roadmap

Based upon the findings from the compliance risk Health/Public Health Compliance Roadmap assessment, the vendor shall support in creating roadmap and implementation plan to address gap findings. The roadmap and implementation plan should include:

- Risk Prioritization (RFO Requirements C.1) - Assess all identified risks and evaluate their level of impact in relation to regulatory requirements and DHHS, OIG, and CMS compliance best practices.
- Compliance Workplan (RFO Requirements B.4, C.1, C.2) - A comprehensive document outlining the steps HCPH must take to mitigate identified risks and address identified gaps and will serve as the foundation for the subsequent enablement of the Healthcare/Public Health Compliance Program, in alignment to the OIG's seven elements.

- Implementation Plan (RFO Requirements C.3, C.4) - The Implementation Plan will provide a timeline for HCPH to execute the high-priority risk mitigation activities and Compliance Workplan milestones. Methods for ongoing monitoring will be incorporated.

1.1.4. Privacy and Security Risk Assessment

Vendor will support, in partnership with the County Attorney's Office (CAO) and the CIO, to identify all health privacy and health-related security risks based on applicable local, state, and Federal laws, regulations, and policies. The risk assessment should include:

- Privacy and Security Program Assessment - Identify security and privacy risks and compliance gaps.
  - Compliance catalogue (RFO Requirements D.1, D.6, D.3a-e, D.4a-m) - Catalogue relevant federal, state and local privacy and security requirements
  - Current state assessment (RFO Requirements D.1, D.2e-I, D.2n-s, D.2w, D.3a-e, D.4a-m, D.5a-c, D.2v) - Understand current privacy and security controls environment and document gaps against requirements. Review network diagrams and similar artifacts at a high level to identify areas of weakness
  - Risk assessment (RFO Requirements D.1, D.6, D.3a-e, D.4a-m) - Analyze current state against relevant adversarial and non-adversarial threats to identify, score and prioritize risks
  - Future state - Design future state profile and develop prioritized recommendations for mitigating risks. Document action items in POAMs.
- ~~Red Team Assessment (RFO Requirements D.2c-d, D.2j-m, D.2t-u, D.5) - Perform technical testing to identify and exploit vulnerabilities in people, processes and technologies.~~
  - ~~Planning - Identify trophies / objectives~~
  - ~~Discovery - Develop footprint of the network~~
  - ~~Vulnerability identification - Perform vulnerability scans of in-scope assets to identify opportunities for exploit~~
  - ~~Exploitation - Exploit vulnerabilities in people, processes and technologies to gain a foothold of the network escalate privileges and achieve objectives~~
  - ~~Reporting - Document findings and available mitigations.~~
- Application Penetration Test (RFO Requirements D.2c-d, D.2l, D.2u)- Perform technical testing to identify and exploit vulnerabilities in applications.
  - Planning - Identify target applications
  - Discovery - Understand application logic
  - Vulnerability identification - Vulnerability scans of in-scope applications to identify opportunities for exploit
  - Exploitation - Exploit application vulnerabilities
  - Reporting - Document findings and available mitigations
- Data cataloging and classification – Catalog and classify data across HCPH applications, and plan for appropriate data protection.
  - Discover and classify data
    - Conduct surveys and targeted interviews to understand data categories and

classifications, attendant regulation (HIPAA, 42 CFR Part2), as well as data locations, formats, lineage and authorized users and uses.

- Document a data security classification standard and protection requirements for each classification level (e.g., encryption, DLP, MFA, etc.).

- Catalog data
  - Create a data catalog that includes data asset name, description, owner, locations, format, lineage, security classification, authorized users and uses, and data retention requirements.
- Plan to protect data and minimize unnecessary PII/PHI
  - Assess each data asset's lifecycle to identify gaps in control coverage based on assigned classification.
  - Identify opportunities to minimize PII/PHI thru tokenization or retention policies.
  - Develop a comprehensive plan to implement the controls identified.

Note: This change request replaces the Red Team assessment task with the Data cataloging and classification task, at no cost to the County. In performing the security and risk assessment, EY and HCPH agreed that a Red Team assessment would only provide short-term value because it would identify point-in-time findings. The EY and HCPH teams identified a more urgent task which would provide longer term value: Data cataloging and classification would help HCPH better understand its data breach risk exposure, and help plan for appropriate data protection.

2. Roles and Responsibilities

County Responsibilities:

- The County will assign a project manager (PM) to oversee the Services provided by the EY team and act as the primary point-of-contact for day-to-day conduct of the project.
- The County will provide timely access to key data, existing policies, and procedures within all pertinent departments during the compliance program project.
- The County will provide timely access to key stakeholders for interviews and discussion.
- Once we conclude the compliance roadmap and the privacy/security risk assessments, our focus will be on enabling the County to remediate gaps and take on steady state operations. For cybersecurity, the HCPH IT and US teams will remediate the gaps as identified in the POA&Ms.
- The county will be responsible for their employee training and education associated with the compliance program implementation. The County will ensure proper and timely certification of compliance and risk management training for employees, vendors, and governing authorities. EY will provide the training plan but it will be the County's responsibility to execute.
- The County will be responsible for all compliance program monitoring and reporting, during and post compliance program implementation. EY will provide the monitoring and reporting plan, but it will be the County's responsibility to execute.
- The County will ensure proper and timely certification of all applicable Harris County employees, and thorough HIPPA/PHI training for all employees. EY will provide the training plan, but it would be the County's responsibility to execute.

Vendor Responsibilities:

- The EY team will perform the activities stated within this SoW and will submit the deliverables within the stated timeline.
- We will provide weekly status reports and attend weekly status review meetings.
- We will hold monthly deliverable reviews to solicit feedback and align with stakeholder objectives.
- We will assign a Project Manager (PM) to lead the delivery of services within this SoW. This person will act as the primary EY point-of-contact for the County.
- We will expeditiously escalate to the County PM any issues that impede the conduct of the project, including lack of access to County stakeholders or subject matter experts.
- Once we conclude the compliance roadmap and the privacy/security risk assessments, our focus will be on enabling the County to remediate gaps and take on steady state operations.

3. Assumptions and Limitations:

Assumptions:

- On-site presence of vendor personnel will be on an as-needed basis. Vendor personnel shall perform their project duties from a remote work location where such performance does not impact deliverable quality.
- Workstreams are not mutually independent and will share dependencies; resources will be shared as needed.
- If and when County requests changes to the scope or processes described here, Vendor shall perform an impact assessment and communicate the impact on results, timeline, and price to the County. Changes will be in effect upon joint agreement via the Change Order Process.
- Vendor and the County will mutually agree when applicable, to a change order for a particular workstream, as needed. All change order(s) shall be subject to the Change Order Process identified within vendor's executed Agreement.

Limitations:

Vendor shall not identify, address, or correct any errors or defects in the County computer systems, other devices, or components thereof ("Systems"), whether due to imprecise or ambiguous entry, storage, interpretation, processing or reporting of data.

Unless stated in the SOW or Change Order, Vendor shall not:

- Perform ongoing internal control monitoring activities or other control activities that affect the execution of transactions or ensure that transactions are properly executed and/or accounted for or perform routine activities in connection with the County's operating or production processes that are equivalent to those of an ongoing compliance or quality control function.
- Perform routine activities in connection with the County's financial processes that are equivalent to those of an ongoing compliance or quality control function.
- Determine which, if any, recommendations for improving internal controls should be implemented.
- Act on your behalf in reporting to your Board of Directors or Audit Committee.

4. Deliverables

4.1. Description of Deliverables

#	Deliverable	Description
MD1 (Once, at the end of month 3)	Health/Public Health Compliance risk assessment	Current State Assessment Documentation (Regulatory Compliance Catalogue, Compliance Landscape, Gap Analysis, Risk Assessment)
MD2 (Once, at the end of month 4)	Health/Public Health	Compliance Roadmap Documentation (Risk Prioritization Document, Compliance Workplan and Implementation Plan)

#	Deliverable	Description
	Compliance roadmap	
MD3 (Monthly, through months 5-12)	Health/Public Health Compliance program development	Enablement Plan Documentation (Controls framework, policies and procedures, monitoring & management plan, training plan, documentation updates)
MD5 (Once, at the end of month 3)	Privacy and Security Assessment	Privacy and Security Program Assessment Report
~~**MD7 (Once, at the end of month 4)**~~		~~Red Team Assessment Report~~
MD8 (Once, at the end of month 5)		Application Penetration Test Report
MD9 (Once, at the end of month 12)	Data classification standard	Standard which describes sensitive data types held and protection requirements for each
MD10 (Once, at the end of month 12)	Data catalog	Inventory of sensitive data types and relevant meta data including data asset name, description, owner, locations, format, lineage, security classification, authorized users and uses, and data retention requirements
MD11 (Once, at the end of month 12)	Data protection plan	Roadmap for implementing required data protection requirements for each data classification

4.2. Format of deliverables

Deliverables shall be formatted as Microsoft Word, Excel or PowerPoint documents.

4.3. Acceptance Criteria

Each deliverable will go through a monthly review before submission. The vendor shall address any feedback received during the review, and will schedule a final review, if required. The acceptance criteria would be deemed met if the deliverable fulfills the scope in this SOW, and if the feedback received from the County has been addressed.

4.4. Project Completion Criteria

The project shall be considered complete when the deliverables specified in this SOW has been submitted by vendor to the County, and has met the acceptance criteria stated within section 4.3. Acceptance Criteria.

5. Schedule

The period of performance is anticipated to be twelve (12) months. The County can reduce the duration of this scope of work with a notification to vendor. Per the master service agreement, the vendor has 30 days upon receipt of the notice to discontinue any service provided.

The project schedule is shown below. As per the County's request, Workstream B will commence on 8/1/23 and Workstream D will start on 9/1/23. Workstream C and A will start once pre-requisite activities have been completed.

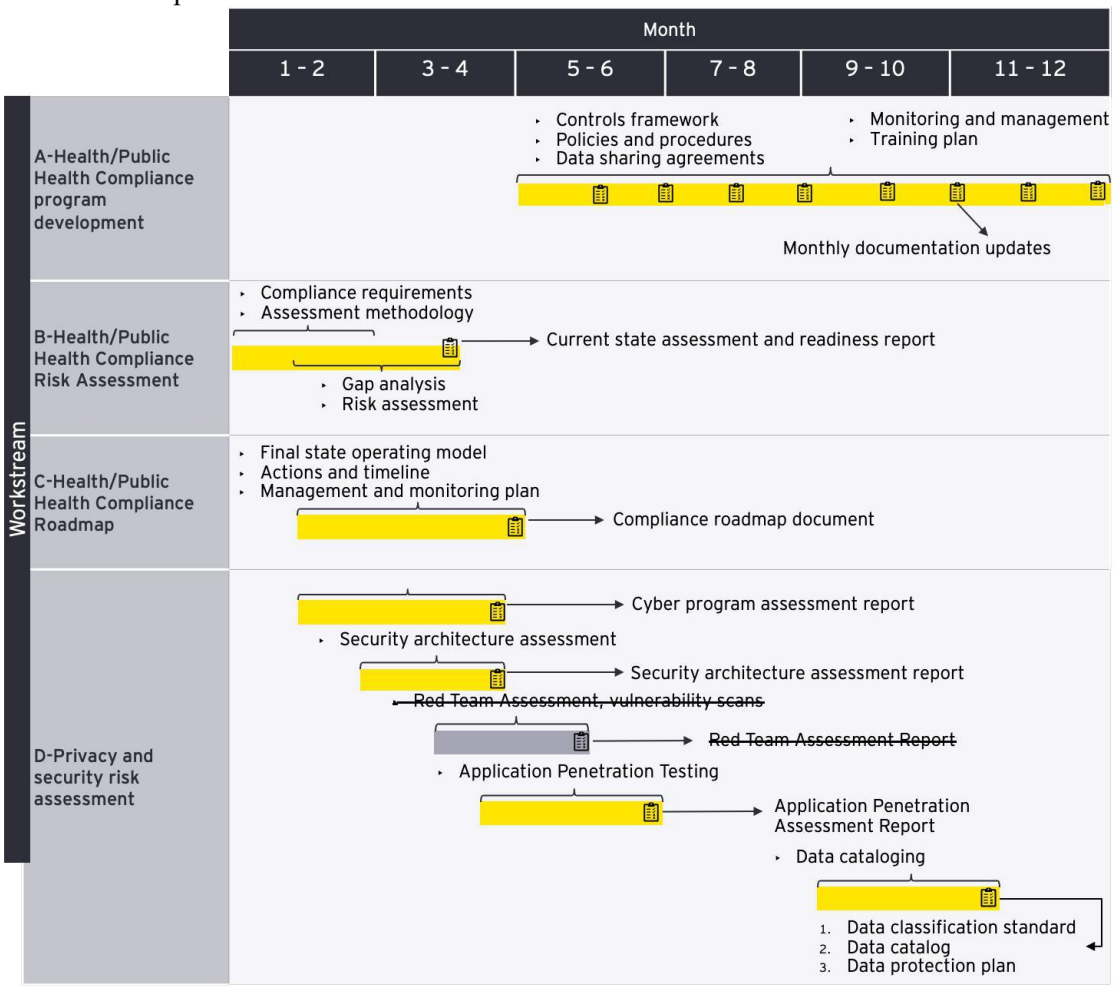

Figure 1: Project schedule

6. Key Personnel

The following are designated Key Personnel for the performance of this SOW.

Name	Project role
Subhankar Sarkar	Delivery Executive
Rakesh Thakur	Cyber Security Lead
Luwanna LaPole	Compliance Lead
Essex De Guzman	Program Manager
Amrutha Krishnaraj	Senior Governance and Compliance Analyst
Tom Herbert	Cybersecurity Analyst

7. Invoices

Refer to vendor's executed Agreement (Job No. 210317 or Job No. 150242).

8. Fees

8.1. Schedule

The total not-to-exceed price for the work performed under this SOW is $1,867,500. This includes all Fixed Price and T&M deliverables. The fee schedule is specified in the table below. Travel costs are included in the not-to-exceed price and are not billed separately.

Deliverable and estimated schedule	**Workstream**	**Deliverable**	**Price Type**	**Quantity**	**Total Price**
MD1 (Once, at the end of month 3)	B-Health/Public Health Compliance risk assessment	Current State Assessment (Risk assessment and Gap analysis) Report	Fixed Price	1	$278,283
MD2 (Once, at the end of month 4)	C-Health/Public Health Compliance roadmap	Compliance Roadmap Document (Compliance Workplan Framework and Implementation Plan)	Fixed Price	1	$139,557
MD3 (Monthly, through months 5-12)	A-Health/Public Health Compliance program development	Enablement Plan (Compliance Workplan, Controls framework, Policies and procedures, Monitoring & management plan, Training Plan~~,~~ Documentation updates)	Time and Material	8	$849,660
MD5 (Once, at the end of month 3)	D-Privacy and Security Assessment	Privacy and Security Program Assessment Report	Fixed Price	1	$300,000
~~MD7 (Once, at the end of month 4)~~	~~D-Privacy and Security Assessment~~	~~Red Team Assessment Report~~	~~Fixed Price~~	~~1~~	~~$175,000~~
MD8 (Once, at the end of month 5)	D-Privacy and Security Assessment	Application Penetration Testing Report	Fixed Price	1	$125,000
MD**9** (Once, at the end of month **12**)	D-Privacy and Security Assessment	Data classification standard	Fixed Price	1	$30,000
MD**10** (Once, at the end of month **12**)	D-Privacy and Security Assessment	Data catalog	Fixed Price	1	$95,000

MD**11** (Once, at the end of month **12**)	D-Privacy and Security Assessment	Data protection plan	Fixed Price	1	$50,000
				Total Fees	**$1,867,500**

8.2. Rate Card

The rate card and estimated hours for T&M deliverables are presented in the table below.

Deliverable	**Labor Category**	**Hourly Rate**	**Hours**	**Total Price**
MD3 - Health/Public Health Compliance program development (5-12 Months)	Strategy Principal III	$360.00	398	$143,280
MD3 - Health/Public Health Compliance program development (5-12 Months)	Strategy Principal II	$340.00	40	$13,600
MD3 - Health/Public Health Compliance program development (5-12 Months)	Research and Analysis PM	$229.00	1400	$320,600
MD3 - Health/Public Health Compliance program development (5-12 Months)	Research and Analysis Associate II	$163.00	1,020	$166,260
MD3 - Health/Public Health Compliance program development (5-12 Months)	Research and Analysis Associate I	$143.00	1,440	$205,920