COUNTY OF SONOMA

575 ADMINISTRATION
DRIVE, ROOM 102A
SANTA ROSA, CA 95403

SUMMARY REPORT

Agenda Date: 12/7/2021

To: Board of Supervisors of Sonoma County
Department or Agency Name(s): Department of Health Services; Information Systems Department, Human Services Department, County Counsel, Human Resources Department
Staff Name and Phone Number: Tina Rivera, 565-7876; John Hartwig; Angela Struckmann; Robert Pittman; Christina Cramer
Vote Requirement: Majority
Supervisorial District(s): Countywide

Title:
Countywide Health Information Security Risk Assessment Agreement

Recommended Action:
Authorize the Director of Health Services, or designee, to execute an agreement with Security Compliance Associates to conduct a health information security risk assessment on the County's Health Insurance Portability and Accountability Act covered components to identify risks and vulnerabilities to protected health information for the period December 1, 2021 through June 30, 2022 in an amount not to exceed $120,400.

Executive Summary:
As a healthcare provider, the County is subject to various state and federal laws protecting client health information. The most notable law is the Health Insurance Portability and Accountability Act, commonly known as HIPAA. These laws require the County to safeguard the confidentiality, integrity, and availability of patient information that is created, used, and/or stored by the Department of Health Services, the Human Services Department, the Human Resources Department, the Information Systems Department, and the Sonoma County Counsel's Office.

HIPAA requires the County to periodically conduct a highly complex and technical analysis of systems and practices to identify risks and vulnerabilities. Because the security risk assessment is a legally required audit requiring independence and specialized expertise, contracting with a professional, experienced company that specializes in this work is critical to ensuring credibility in the final report. Jointly, the County's Healthcare Privacy and Security Officer and the Department of Health Services' Compliance Officer have determined that a conducting a HIPAA security risk assessment is a high-priority compliance item.

In April 2019 the County issued a request for proposals (RFP) to conduct a comprehensive HIPAA security risk assessment. The lowest responsive bidder, Security Compliance Associates, was selected, and they successfully completed the assessment in Fall of 2019. Because Security Compliance Associates was the lowest responsive bidder in 2019, and in order to maintain standardization between the last assessment and this next assessment, the General Services Department Purchasing Agent has approved a single-source waiver for this contract.

County staff involvement includes participation by the Information Systems Department, the Human Services Department, the Department of Health Services, County Human Resources, and by the County Counsel's office.

Discussion:

As an entity that provides health care and holds patient's protected health information, the County is subject to provisions of several laws governing protection of client information including the Health Insurance Portability and Accountability Act of 1996, augmented by the Health Information Technology for Economic and Clinical Health Act of 2009, collectively known as HIPAA/HITECH. These laws require the County to safeguard the confidentiality, integrity, and availability of patient information that is created, used, and/or stored primarily in the Department of Health Services, but also to a lesser extent in the Human Services Department, Human Resources Department, Information Systems Department, and the Sonoma County Counsel's Office. These safeguards may be in the form of systems, policies, procedures, and other appropriate security measures.

One of the measures required by HIPAA/HITECH is a risk assessment, which consists of a thorough and accurate evaluation of the risks and vulnerabilities to protected health information (See 45 CFR § 164.308(a)(1)(ii)(A)). Conducting a risk assessment acts as an audit to help the County identify vulnerabilities and implement safeguards that ensure the confidentiality, integrity, and availability of protected health information. The last HIPAA/HITECH security risk assessment conducted by the County was in 2019. Jointly, the County's Healthcare Privacy and Security Officer and the Department of Health Services' Compliance Officer have determined that a current HIPAA/HITECH security risk assessment is a high-priority compliance item.

Conducting a HIPAA/HITECH security risk assessment is a highly complex and technical process that includes specialized information technology system testing and requires a high-level understanding of computer security standards. Because the security risk assessment is a legally required audit intended to identify vulnerabilities to systems and processes, independence and expertise are required of the individual or group conducting the assessment. As such, contracting the risk assessment with a professional, experienced company that specializes in this work is critical to ensuring independence and credibility in the final report.

In April 2019 the County issued a request for proposals to conduct a comprehensive HIPAA/HITECH security risk assessment. The request for proposals required firms to submit a proposal to assess the following four areas: 1) HIPAA risk analysis (evaluate systems), 2) HIPAA security rule gap analysis (evaluate safeguards), 3) HIPAA privacy rule gap analysis (evaluate policies), and 4) HIPAA physical assessment (evaluate physical security). Security Compliance Associates was the lowest cost vendor that could perform all four of the requested risk assessment elements. They worked with County staff to successfully complete the assessment and Security Compliance Associates provided a detailed report to the County on February 13, 2020.

The work that Security Compliance Associates performed demonstrated that they are well qualified and experienced in conducting HIPAA/HITECH security risk assessments in a public sector environment. Because Security Compliance Associates was the lowest responsive bidder in 2019, and in order to maintain standardization between the last assessment and this next assessment, the Department of Health Services requested approval of a single-source waiver from the General Services Department. The single-source request was approved by the Purchasing Agent on October 6, 2021.

County staff involvement will include participation by network and security staff in the Information Systems Department, information technology staff in the Human Services Department, privacy staff in the Department of Health Services, and legal analysis by the County Counsel's office. Additional staff involvement will be required for evaluation of health information security practices in the Human Resources Department and the Sonoma County Counsel's Office. The Department anticipates completion of final security risk assessment reports in April 2022.

Agenda Date: 12/7/2021

Strategic Plan:
Conducting the HIPAA/HITECH security risk assessment supports the County's goal of a Healthy and Safe Community by ensuring that client health information is protected. In addition to alignment with the County's Strategic Plan, this project supports the Department's Strategic Plan goal of being a high-achieving, high-functioning organization with effective and efficient administrative functions. Completion of the HIPAA/HITECH security risk assessment will bring the County into compliance with this high-risk element of HIPAA compliance.

This item directly supports the County's Five-year Strategic Plan and is aligned with the following pillar, goal, and objective.

> **Pillar:** Healthy and Safe Communities
> **Goal:** Goal 1: Strengthen operational effectiveness, fiscal reliability, and accountability
> **Objective:** Objective 2: Identify gaps in the Safety Net system of services and identify areas where departments can address those gaps directly, and seek guidance from the Board when additional resources and/or policy direction is needed.

Prior Board Actions:
None

FISCAL SUMMARY

Expenditures	**FY 21-22 Adopted**	**FY 22-23 Projected**	**FY 23-24 Projected**
Budgeted Expenses	90,300		
Additional Appropriation Requested	30,100		
Total Expenditures	**120,400**	**0**	**0**
Funding Sources			
General Fund/WA GF			
State/Federal	120,400		
Fees/Other			
Use of Fund Balance			
Contingencies			
Total Sources	**120,400**	**0**	**0**

Narrative Explanation of Fiscal Impacts:
The contract expense will be shared between DHS $90,300 & HSD $30,100 for a total of $120,400. Health Services has $90,300 budgeted in FY 2021-2022 and will be funded through 1991 Realignment. Human Services will fund the allotted portion of $30,100 using fund balance, and will add the appropriations as part of the upcoming Q2 Consolidated Budget Adjustment.

Staffing Impacts:

Position Title (Payroll Classification)	Monthly Salary Range (A-I Step)	Additions (Number)	Deletions (Number)

Narrative Explanation of Staffing Impacts (If Required):
N/A

Attachments:
Attachment 1 - Agreement with Security Compliance Associates

Related Items "On File" with the Clerk of the Board:
None