Legislation Text

File #: 2019-1176, **Version:** 1

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: Barbie Robinson, 565-7876; John Hartwig; Karen Fies; Bruce Goldstein, 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 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 August 15, 2019 through June 30, 2020 in an amount not to exceed $125,100.

Executive Summary:
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 periodic analysis of systems and practices to identify risks and vulnerabilities to protected health information. Conducting a HIPAA/HITECH security risk assessment is a highly complex and technical process that includes specialized system review. Because the security risk assessment is a legally required audit requiring independence and specialized expertise, contracting the risk assessment with a professional, experienced company that specializes in this work is critical to ensuring credibility in the final report. The last HIPAA/HITECH security risk assessment conducted by the County was in 2011. 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.

In April 2019 the County issued a request for proposals to conduct a comprehensive HIPAA/HITECH security risk assessment including HIPAA risk analysis (evaluates systems), HIPAA security rule gap analysis (evaluates safeguards), HIPAA privacy rule gap analysis (evaluates policies), and a HIPAA physical assessment (evaluates

physical security). Fourteen qualified companies submitted bids that were evaluated by a team of five subject matter experts from Department of Health Services, Human Services Department, and Information Systems Department. After review of the bidder submissions, the evaluation team recommends Security Compliance Associates as the contractor to conduct the HIPAA/HITECH security risk assessment. Security Compliance Associates was the lowest cost vendor that can perform all four of the requested risk assessment elements and they are well qualified and experienced in conducting HIPAA/HITECH security risk assessments in a public sector environment.

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.

Discussion:
As an entity that provides health care and holds patient's protected health information, Sonoma County is subject to provisions of 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. Under HIPAA/HITECH the County is required 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 2011. 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 conduct an assessment of 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). In response to the request for proposals, 14 qualified companies submitted bids. The bids were evaluated by a team of five subject matter experts from the Department of Health Services, Human Services Department, and Information Systems Department. The evaluation was conducted consistent with County policy.

Security Compliance Associates was the lowest cost vendor that can perform all four of the requested risk assessment elements. They submitted a complete request for proposals response that met all request for

proposals standards. Security Compliance Associates demonstrated that they are well qualified and experienced in conducting HIPAA/HITECH security risk assessments in the public sector. The County evaluation team interviewed five Security Compliance Associates managers and staff to clarify questions about Security Compliance Associates' response and to ensure that Security Compliance Associates is qualified to perform the work. The evaluation team collectively agreed that Security Compliance Associates is highly qualified. As a result of the evaluation process, the evaluation team recommends Security Compliance Associates as the contractor to conduct the HIPAA/HITECH security risk assessment.

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 December 2019.

Strategic Plan Alignment - Conducting the HIPAA/HITECH security risk assessment supports the County's goal of a Safe, Healthy, and Caring 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.

Prior Board Actions:
None

FISCAL SUMMARY

Expenditures	**FY 19-20 Adopted**	**FY 20-21 Projected**	**FY 21-22 Projected**
Budgeted Expenses			
Additional Appropriation Requested	125,100		
Total Expenditures	**125,100**	**0**	**0**
Funding Sources			
General Fund/WA GF			
State/Federal			
Fees/Other	125,100		
Use of Fund Balance			
Contingencies			
Total Sources	**125,100**	**0**	**0**

Narrative Explanation of Fiscal Impacts:
Funding of $125,100 for the HIPAA/HITECH security risk assessment agreement will be added to the FY 19-20 budget via the consolidated budget adjustments process. The funding source for the agreement is Intergovernmental Transfer funding.

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:
Agreement with Security Compliance Associates

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