

COUNTY OF SONOMA  
AGREEMENT FOR SERVICES

This agreement ("Agreement"), dated as of \_\_\_\_\_, 2019 ("Effective Date"), is by and between the County of Sonoma, a political subdivision of the State of California (hereinafter "County"), and Security Compliance Associates, an information security consulting agency (hereinafter "Contractor").

R E C I T A L S

WHEREAS, the County, as a provider of health care services, is required under the Health Insurance Portability and Accountability Act of 1996, known as HIPAA, to conduct a periodic assessment of systems and practices to identify risks and vulnerabilities to protected health information;

WHEREAS, protected health information subject to HIPAA is created, used and/or stored in the following departments: Department of Health Services, Human Services Department, Human Resources Department, Information Services Department, and County Counsel;

WHEREAS, the Department of Health Services seeks to engage Contractor to perform a security risk assessment of all protected health information in the County under the direction of the Office of County Counsel;

WHEREAS, Contractor represents that it has expertise and broad experience performing information security risk assessments and providing compliance advisory services; and

WHEREAS, in the judgment of the Board of Supervisors, it is necessary and desirable to use the services of Contractor to perform a security risk assessment and other services described in RFP 19-001, consistent with standards established by the U.S. Department of Health and Human Services and in compliance with Federal and State regulations including HIPAA and HITECH (Health Information Technology for Economic and Clinical Health Act of 2009).

NOW, THEREFORE, in consideration of the foregoing recitals and the mutual covenants contained herein, the parties hereto agree as follows:

A G R E E M E N T

1. Scope of Services

1.1. Contractor's Specified Services

Contractor shall perform the services described in Exhibit A (Scope of Work and Budget), attached hereto and incorporated herein by this reference (hereinafter "Exhibit A"), within the times or by the dates provided for in Exhibit A and pursuant to Article 7 (Prosecution of Work). In the event of a conflict between the body of this Agreement and Exhibit A, the provisions in the body of this Agreement shall control.

1.2. Cooperation With County

Contractor shall cooperate with County and County staff in the performance of all work hereunder.

1.3. Performance Standard

Contractor shall perform all work hereunder in a manner consistent with the level of competency and standard of care normally observed by a person practicing in Contractor's profession. County has relied upon the professional ability and training of Contractor as a material inducement to enter into this Agreement. Contractor hereby agrees to provide all services under this Agreement in accordance with generally accepted professional practices and standards of care, as well as the requirements of applicable federal, state, and local laws, it being understood that acceptance of Contractor's work by County shall not operate as a waiver or release. If County determines that any of Contractor's work is not in accordance with such level of competency and standard of care, County, in its sole discretion, shall have the right to do any or all of the following: (a) require Contractor to meet with County to review the quality of the work and resolve matters of concern; (b) require Contractor to repeat the work at no additional charge until it is satisfactory; (c) terminate this Agreement pursuant to the provisions of Article 4 (Termination); or (d) pursue any and all other remedies at law or in equity.

1.4. Assigned Personnel

- a. Contractor shall assign only competent personnel to perform work hereunder. In the event that at any time County, in its sole discretion, desires the removal of any person or persons assigned by Contractor to perform work hereunder, Contractor shall remove such person or persons immediately upon receiving written notice from County.
- b. Any and all persons identified in this Agreement or any exhibit hereto as the project manager, project team, or other professional performing work hereunder are deemed by County to be key personnel whose services were a material inducement to County to enter into this Agreement, and without whose services County would not have entered into this Agreement. Contractor shall not remove, replace, substitute, or otherwise change any key personnel without the prior written consent of County.
- c. In the event that any of Contractor's personnel assigned to perform services under this Agreement become unavailable due to resignation, sickness, or other factors outside of Contractor's control, Contractor shall be responsible for timely provision of adequately qualified replacements.

1.5. Contract Exhibits

This Agreement includes the following exhibits, which are hereby incorporated by reference as though fully set forth herein:

- Exhibit A. Scope of Work and Budget
- Exhibit B. Insurance Requirements
- Exhibit C. Business Associate Addendum

2. Payment

For all services and incidental costs required hereunder, Contractor shall be paid in accordance with the following terms:

2.1. Payment for Services

Contractor shall be paid in multiple lump sums in accordance with Exhibit A (Scope of Work and Budget), attached hereto and incorporated herein by this reference (hereinafter "Exhibit A"), regardless of the number of hours or length of time necessary for Contractor to complete the services. Contractor shall not be entitled to any additional payment for any expenses incurred in completion of the services. Exhibit A includes a breakdown of costs used to derive the lump sum amount, including but not limited to hourly rates, estimated travel expenses, and other applicable rates.

Upon completion of the work, Contractor shall submit its bill[s] for payment in a form approved by County's Auditor and the Head of County department receiving the services. The bill[s] shall identify the services completed and the amount charged.

Unless otherwise noted in this Agreement, payments shall be made within the normal course of County business after presentation of an invoice in a form approved by County for services performed. Payments shall be made only upon the satisfactory completion of the services as determined by County.

2.2. Maximum Payment Obligation

In no event shall County be obligated to pay Contractor more than the total sum of \$125,100 under the terms and conditions of this Agreement.

2.3. California Franchise Tax Withhold

Pursuant to California Revenue and Taxation Code (R&TC) Section 18662, County shall withhold seven percent of the income paid to Contractor for services performed within the State of California under this Agreement for payment and reporting to the California Franchise Tax Board if Contractor does not qualify as: (1) a corporation with its principal place of business in California, (2) an LLC or partnership with a permanent place of business in California, (3) a corporation/LLC or partnership qualified to do business in California by the Secretary of State, or (4) an individual with a permanent residence in the State of California.

If Contractor does not qualify, County requires that a completed and signed California Form 587 be provided by Contractor in order for payments to be made. If Contractor is qualified, then County requires a completed California Form 590. California Forms 587 and 590 remain valid for the duration of the Agreement provided there is no material change in facts. By signing either form, Contractor agrees to promptly notify County of any changes in the facts. Forms should be sent to County pursuant to Article 13 (Method and Place of Giving Notice, Submitting Bills, and Making Payments). To reduce the amount withheld, Contractor has the option to provide County with either a full or partial waiver from the State of California.

2.4. Overpayment

If County overpays Contractor for any reason, Contractor agrees to return the amount of such overpayment to County, or at County's option, permit County to offset the amount of such overpayment against future payments owed to Contractor under this Agreement or any other agreement.

2.5. Disallowance of Payment

In the event that Contractor claims or receives payment from County for a service, reimbursement for which is later disallowed by County, State of California, or the United States Government, then Contractor shall promptly refund the disallowed amount to County upon request, or at its option, County may offset the amount disallowed from any payment due or that becomes due to Contractor under this Agreement or any other agreement.

2.6. Budget Line Amendments

County Department of Health Services Director is authorized to approve and execute a "Budget Revision Form", which revises program funds in the line items set forth in the Program Budget Summary, so long as changes do not result in an increase in County's maximum payment obligation as set forth in Article 2 (Payment) of this Agreement.

2.7. Federal Funding

This Section 2.7 is applicable if all or part of this Agreement will be paid with federal awards.

2.7.1. Required Information

As a pass-through entity, County is required to provide certain information regarding federal award(s) to Contractor as a subrecipient. In signing this Agreement, Contractor acknowledges receipt of the following information regarding federal award(s) that will be used to pay this Agreement:

- a. CFDA Number:
- b. CFDA Title:
- c. Federal Agency:
- d. Award Name:
- e. Federal Award(s) Amount:

2.7.2. Title 2 Code of Federal Regulations Part 200

As a subrecipient of federal awards, Contractor is subject to the provisions of Title 2 Code of Federal Regulations Part 200 Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (hereinafter "2 CFR Part 200"). In signing this Agreement, Contractor acknowledges that it understands and will comply with the provisions of 2 CFR Part 200. One provision of 2 CFR Part 200 requires a subrecipient that expends \$750,000 in federal awards during its fiscal year to have an audit performed in accordance with 2 CFR Part 200. If such an audit is required, Contractor agrees to provide County with a copy of the audit report within 9 months of Contractor's fiscal year-end. Questions regarding 2 CFR Part 200 can be directed to County's Auditor-Controller-Treasurer-Tax Collector's Office – General Accounting Division.

2.7.3. Audits

Contractor agrees that all expenditures of state and federal funds furnished to Contractor pursuant to this Agreement are subject to audit by County, state agencies, and/or federal agencies. Contractor warrants that it shall comply with the audit requirements as set forth in 2 CFR Part 200. County agrees to provide 14-days notice of intent of County to audit

Contractor. Contractors subject to the Single Audit Act of 1984 and Single Audit Act Amendments of 1996 shall annually submit an independent audit conforming to 2 CFR Part 200, which applies to non-profit organizations.

2.7.4. Copy of Audit

Contractor agrees that a copy of audits performed shall be submitted to County no later than 30 days after completion of the audit report, or no later than 9 months after the end of Contractor's fiscal year, whichever comes first. The Contractor's agreement(s) with audit firms shall have a clause to permit access by County, state agencies, and/or federal agencies to the working papers of the external independent auditor.

2.7.5. Retention of Audit Report

Contractor agrees that audit reports and work papers shall be retained for a minimum of 7 years from the date of the audit report, unless the auditor is notified in writing by County, a state agency, and/or a federal agency to extend the retention period.

2.7.6. Repayment

Contractor is responsible for the repayment of all audit exceptions and disallowances taken by County, state agencies, and/or federal agencies related to services provided by Contractor under this Agreement. Unallowable costs that have been claimed and reimbursed will be refunded to the program that reimbursed the unallowable costs either by cash refund or by offset to subsequent claims.

3. Term of Agreement

The term of this Agreement shall be from Effective Date to June 30, 2020 unless terminated earlier in accordance with the provisions of Article 4 (Termination).

4. Termination

4.1. Termination Without Cause

Notwithstanding any other provision of this Agreement, at any time and without cause, County shall have the right, in its sole discretion, to terminate this Agreement by giving 5 days advance written notice to Contractor.

4.2. Termination for Cause

Notwithstanding any other provision of this Agreement, should Contractor fail to perform any of its obligations hereunder within the time and in the manner herein provided or otherwise violate any of the terms of this Agreement, County may immediately terminate this Agreement by giving Contractor written notice of such termination, stating the reason for termination.

4.3. Delivery of Work Product and Final Payment Upon Termination

In the event of termination, Contractor, within 14 days following the date of termination, shall deliver to County all materials and work product subject to Section 10.13 (Ownership and Disclosure of Work Product) and all reports, original drawings, graphics, plans, studies, and other data or documents, in whatever form or format, assembled or prepared by Contractor or Contractor's subcontractors, consultants, and other agents in connection with this Agreement, and shall submit to County an invoice showing the services performed, hours worked, and copies of receipts for reimbursable expenses up to the date of termination.

4.4. Payment Upon Termination

Upon termination of this Agreement by County, Contractor shall be entitled to receive, as full payment for all services satisfactorily rendered and reimbursable expenses properly incurred hereunder, an amount which bears the same ratio to the total payment specified in the Agreement as the services satisfactorily rendered hereunder by Contractor bear to the total services otherwise required to be performed for such total payment; provided, however, that if services which have been satisfactorily rendered are to be paid on a per-hour or per-day basis, Contractor shall be entitled to receive as full payment an amount equal to the number of hours or days actually worked prior to the termination times the applicable hourly or daily rate; and further provided, however, that if County terminates the Agreement for cause pursuant to Section 4.2 (Termination for Cause), County shall deduct from such amount the amount of damage, if any, sustained by County by virtue of the breach of the Agreement by Contractor.

4.5. Authority to Terminate

The Board of Supervisors has the authority to terminate this Agreement on behalf of County. In addition, the Purchasing Agent or Department of Health Services' Head, in consultation with County Counsel, shall have the authority to terminate this Agreement on behalf of County.

4.6. Obligations After Termination

The following shall remain in full force and effect after termination of this Agreement: (1) Section 2.7 (Federal Funding), (2) Article 5 (Indemnification), (3) Section 10.7 (Records Maintenance), (4) Section 10.7.1 (Right to Audit, Inspect, and Copy Records), (5) Section 10.17 (Confidentiality), and (6) Section 14.5 (Applicable Law and Forum).

4.7. Change in Funding

Contractor understands and agrees that County shall have the right to terminate this Agreement immediately upon written notice to Contractor in the event that (1) any state and/or federal agency and/or other funder(s) reduces, withholds, or terminates funding which County anticipated using to pay Contractor for services provided under this Agreement, or (2) County has exhausted all funds legally available for payments due under this Agreement.

5. Indemnification

Contractor agrees to accept all responsibility for loss or damage to any person or entity, including County, and to indemnify, hold harmless, and release County, its officers, agents, and employees from and against any actions, claims, damages, liabilities, disabilities, or expenses that may be asserted by any person or entity, including Contractor, that arise out of, pertain to, or relate to Contractor's or its agents', employees', contractors', subcontractors', or invitees' performance or obligations under this Agreement. Contractor agrees to provide a complete defense for any claim or action brought against County based upon a claim relating to such Contractor's or its agents', employees', contractors', subcontractors', or invitees' performance or obligations under this Agreement. Contractor's obligations under this Article apply whether or not there is concurrent or contributory negligence on County's part, but to the extent required by law, excluding liability due to County's conduct. County shall have the right to select its legal counsel at Contractor's expense, subject to Contractor's approval, which shall not be unreasonably withheld. This indemnification obligation is not limited in any way by any

limitation on the amount or type of damages or compensation payable to or for Contractor or its agents under workers' compensation acts, disability benefits acts, or other employee benefit acts.

6. Insurance

With respect to performance of work under this Agreement, Contractor shall maintain and shall require all of its subcontractors, consultants, and other agents to maintain insurance as described in Exhibit B (Insurance Requirements), which is attached hereto and incorporated herein by this reference (hereinafter "Exhibit B").

7. Prosecution of Work

The execution of this Agreement shall constitute Contractor's authority to proceed immediately with the performance of this Agreement. Performance of the services hereunder shall be completed within the time required herein, provided, however, that if the performance is delayed by earthquake, flood, high water, or other Act of God, or by strike, lockout, or similar labor disturbances, the time for Contractor's performance of this Agreement shall be extended by a number of days equal to the number of days Contractor has been delayed.

8. Extra or Changed Work

Extra or changed work or other changes to the Agreement may be authorized only by written amendment to this Agreement, signed by both parties. Changes which do not exceed the delegated signature authority of the Department may be executed by the Department Head in a form approved by County Counsel. The Board of Supervisors or Purchasing Agent must authorize all other extra or changed work which exceeds the delegated signature authority of the Department Head. The parties expressly recognize that, pursuant to Sonoma County Code Section 1-11, County personnel are without authorization to order extra or changed work or waive Agreement requirements. Failure of Contractor to secure such written authorization for extra or changed work shall constitute a waiver of any and all right to adjustment in the Agreement price or Agreement time due to such unauthorized work and thereafter Contractor shall be entitled to no compensation whatsoever for the performance of such work. Contractor further expressly waives any and all right or remedy by way of restitution and quantum meruit for any and all extra work performed without such express and prior written authorization of the County.

9. Representations of Contractor

9.1. Standard of Care

County has relied upon the professional ability and training of Contractor as a material inducement to enter into this Agreement. Contractor hereby agrees that all its work will be performed and that its operations shall be conducted in accordance with generally accepted and applicable professional practices and standards as well as the requirements of applicable federal, state, and local laws, it being understood that acceptance of Contractor's work by County shall not operate as a waiver or release.

9.2. Status of Contractor

The parties intend that Contractor, in performing the services specified herein, shall act as an independent contractor and shall control the work and the manner in which it is performed. Contractor is not to be considered an agent or employee of County and is not entitled to participate in any pension plan, workers' compensation plan, insurance, bonus, or similar benefits

that County provides its employees. In the event County exercises its right to terminate this Agreement pursuant to Article 4 (Termination), Contractor expressly agrees that it shall have no recourse or right of appeal under rules, regulations, ordinances, or laws applicable to employees.

9.3. No Suspension or Debarment

Contractor warrants that it is not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in covered transactions by any federal department or agency. Contractor also warrants that it is not suspended or debarred from receiving federal funds as listed in the "List of Parties Excluded from Federal Procurement or Nonprocurement Programs" issued by the General Services Administration. If Contractor becomes debarred, Contractor has the obligation to inform County.

10. Representation, Warranty, and Responsibility as to Data Security

10.1. Data Security

Contractor shall preserve, and shall ensure that its sub-consultants or vendors preserve, the confidentiality, integrity, and availability of County data with administrative, technical and physical measures that conform to generally recognized industry standards and best practices that the selected firm then applies to its own processing environment. Maintenance of a secure processing environment includes, but is not limited to, the timely application of patches, fixes and updates to operating systems and applications as provided by Contractor and/or its sub-consultants or vendors. Contractor agrees to, and shall ensure that its sub-consultants or vendors, comply with County's current and future information security policies, standards, procedures, and guidelines.

10.2. Encryption Requirements

Contractor shall encrypt, and shall ensure that its sub-consultants or vendors encrypt, confidential information whether the data is in transit, or at rest, including but not limited to Personally Identifiable Information (PII) or Protected Health Information (e.g., PHI, ePHI).

10.3. Security Breach

Contractor shall comply, and shall ensure that its sub-consultants or vendors comply, with all applicable laws that require the notification of individuals in the event of unauthorized release of personally identifiable information(PII) or protected health information(e.g., PHI, ePHI) or other event requiring notification. In the event of a breach, or other event requiring notification under applicable law, Contractor shall:

- a. Notify County by telephone and e-mail within twenty-four (24) hours of any suspected or actual breach of security, intrusion, or unauthorized use or disclosure of information of which Contractor or its agents become aware and/or any actual or suspected use or disclosure of data in violation of any applicable federal or state laws or regulations.
- b. Assume responsibility for informing all such individuals in accordance with applicable federal or state laws or regulations.
- c. Pursuant to Article 5 (Indemnification) of the Agreement, provide indemnity and other protection as specified therein.



10.4. Request to Audit

Contractor will accommodate and upon reasonable notice by Sonoma County, work with Sonoma County and/or its subcontractors to submit to a random information security audit. This is to ensure that the Contractor's and/or Vendor's information security practices or standards comply with Sonoma County's information security policies, standards, procedures and guidelines. Contractor shall ensure that its sub-consultants or vendors comply with this requirement.

10.5. Cyber Risk Insurance Requirements

Contractor shall include, and shall ensure that its sub-contractors or vendors include cyber risk insurance requirements in compliance with County of Sonoma Risk Management standards.

10.6. Taxes

Contractor agrees to file federal and state tax returns and pay all applicable taxes on amounts paid pursuant to this Agreement, and shall be solely liable and responsible to pay such taxes and other obligations, including but not limited to state and federal income and FICA taxes. Contractor agrees to indemnify and hold County harmless from any liability which it may incur to the United States or to the State of California as a consequence of Contractor's failure to pay, when due, all such taxes and obligations. In case County is audited for compliance regarding any withholding or other applicable taxes, Contractor agrees to furnish County with proof of payment of taxes on these earnings.

10.7. Records Maintenance

Contractor shall keep and maintain full and complete documentation and accounting records concerning all services provided under this Agreement. Records shall include all medical records, accounting records, and administrative records related to services provided hereunder. Contractor agrees to preserve and maintain such records for a period of at least 7 years following the close of County and state fiscal year in which the services were provided. If an audit has been started, records must be retained until completion and final resolution of any and all issues that might arise. Final settlement shall be made at the end of the audit and appeal process. All accounting records shall be maintained so that they clearly reflect the source of funding for each type of service for which reimbursement is claimed by Contractor. Accounting records include, but are not limited to, all ledgers, books, vouchers, time sheets, payrolls, appointment schedules, client data cards, and schedules for allocating costs.

10.7.1. Right to Audit, Inspect, and Copy Records

Contractor agrees to permit County and any authorized state or federal agency to audit, inspect, and copy all records, notes, and writings of any kind in connection with the services provided by Contractor under this Agreement, to the extent permitted by law, for the purpose of monitoring the quality and quantity of services, monitoring the accessibility and appropriateness of services, and ensuring fiscal accountability. All such audits, inspections, and copying shall occur during normal business hours. Upon request, Contractor shall supply copies of any and all such records to County. Failure to provide the above-noted documents requested by County within the requested time frame indicated may result in County withholding payments due under this Agreement. In those situations required by applicable law(s), Contractor agrees to obtain necessary releases to permit County or governmental or accrediting agencies to access patient medical records.

10.8. Conflict of Interest

Contractor covenants that it presently has no interest and that it will not acquire any interest, direct or indirect, that represents a financial conflict of interest under state law or that would otherwise conflict in any manner or degree with the performance of its services hereunder. Contractor further covenants that in the performance of this Agreement, no person having any such interests shall be employed. In addition, if requested to do so by County, Contractor shall complete and file and shall require any other person doing work under this Agreement to complete and file a "Statement of Economic Interest" with County disclosing Contractor's or such other person's financial interests.

10.9. Statutory Compliance/Living Wage Ordinance

Contractor agrees to comply, and to ensure compliance by its subconsultants or subcontractors, with all applicable federal, state and local laws, regulations, statutes and policies, including but not limited to the County of Sonoma Living Wage Ordinance, applicable to the services provided under this Agreement as they exist now and as they are changed, amended or modified during the term of this Agreement. Without limiting the generality of the foregoing, Contractor expressly acknowledges and agrees that this Agreement is subject to the provisions of Article XXVI of Chapter 2 of the Sonoma County Code, requiring payment of a living wage to covered employees. Noncompliance during the term of the Agreement will be considered a material breach and may result in termination of the Agreement or pursuit of other legal or administrative remedies.

10.10. Nondiscrimination

Without limiting any other provision hereunder, Contractor shall comply with all applicable federal, state, and local laws, rules, and regulations in regard to nondiscrimination in employment because of race, color, ancestry, national origin, religious creed, belief or grooming, sex (including sexual orientation, gender identity, gender expression, transgender, pregnancy, childbirth, medical conditions related to pregnancy, childbirth or breast feeding), marital status, age, medical condition, physical or mental disability, genetic information, military or veteran status, or any other legally protected category or prohibited basis, including without limitation, the County's Non-Discrimination Policy. All nondiscrimination rules or regulations required by law to be included in this Agreement are incorporated herein by this reference.

10.11. AIDS Discrimination

Contractor agrees to comply with the provisions of Chapter 19, Article II, of the Sonoma County Code prohibiting discrimination in housing, employment, and services because of AIDS or HIV infection during the term of this Agreement and any extensions of the term.

10.12. Assignment of Rights

Contractor assigns to County all rights throughout the world in perpetuity in the nature of copyright, trademark, patent, and right to ideas in and to all versions of the plans and specifications, if any, now or later, prepared by Contractor in connection with this Agreement. Contractor agrees to take such actions as are necessary to protect the rights assigned to County in this Agreement, and to refrain from taking any action which would impair those rights. Contractor's responsibilities under this provision include, but are not limited to, placing proper notice of copyright on all versions of the plans and specifications as County may direct, and refraining from disclosing any versions of the plans and specifications to any third party without

first obtaining written permission of County. Contractor shall not use or permit another party to use the plans and specifications in connection with this or any other project without first obtaining written permission of County.

10.13. Ownership and Disclosure of Work Product

All reports, original drawings, graphics, plans, studies, and other data or documents (“documents”), in whatever form or format, assembled or prepared by Contractor or Contractor's subcontractors, consultants, and other agents in connection with this Agreement, shall be the property of County. County shall be entitled to immediate possession of such documents upon completion of the work pursuant to this Agreement. Upon expiration or termination of this Agreement, Contractor shall promptly deliver to County all such documents which have not already been provided to County in such form or format as County deems appropriate. Such documents shall be and will remain the property of County without restriction or limitation. Contractor may retain copies of the above-described documents, but agrees not to disclose or discuss any information gathered, discovered, or generated in any way through this Agreement without the express written permission of County.

10.13.1. Final Report/Deliverables

The final report and all other documents required to be submitted to the County pursuant to the Scope of Work shall be directed to:

Phyllis Gallagher, Chief Deputy County Counsel  
Office of County Counsel  
575 Administration Drive, #105A  
Santa Rosa, CA. 95403

10.14. Authority

The undersigned hereby represents and warrants that he or she has authority to execute and deliver this Agreement on behalf of Contractor.

10.15. Sanctioned Employee

Contractor agrees that it shall not employ in any capacity, or retain as a subcontractor in any capacity, any individual or entity that is listed on any list published by the Federal Office of Inspector General regarding the sanctioning, suspension, or exclusion of individuals or entities from the federal Medicare and Medicaid programs. Contractor agrees to monthly review said state and federal lists to confirm the status of current employees, subcontractors, and contractors. In the event Contractor does employ such individual(s) or entity(ies), Contractor agrees to assume full liability for any associated penalties, sanctions, loss, or damage that may be imposed on County by the Medicare or Medicaid programs.

10.16. Compliance with County Policies and Procedures

Contractor agrees to comply with all County policies and procedures as they may relate to services provided hereunder, including, but not limited to, County's policies and procedures, manuals, programs, and processes related to selection, retention, credentialing and recredentialing providers, utilization management, quality management, compliance, grievances, appeals, and expedited appeals, advanced directives, and administrative manual.

10.17. Confidentiality

Contractor agrees to maintain the confidentiality of all patient medical records and client information in accordance with all applicable state and federal laws and regulations. This Section 10.17 shall survive termination of this Agreement.

10.18. Lobbying

If any federal funds are to be used to pay for any services under this Agreement, Contractor shall fully comply with all certifications and disclosure requirements prescribed by Section 319 of the Public Law 101-121 (31 United States Code Section 1352) and any implementing regulations, and shall ensure that each of its subcontractors receiving funds under this Agreement also fully complies with all such certification and disclosure requirements.

10.19. Subcontractors

Contractor agrees that any employees or agents of Contractor that assist Contractor in the provision of services shall also satisfy the requirements of this Agreement. In this regard, Contractor understands and agrees that all obligations and prohibitions imposed on Contractor pursuant to this Agreement are equally applicable to each and every individual providing services through Contractor under this Agreement, and Contractor shall assure that such individuals agree to comply with such obligations and prohibitions.

10.20. Licensure and Staffing

Contractor warrants that it and all its employees and sub-contractors providing or supervising services under this Agreement have all necessary licenses, permits, and certificates to provide services under this Agreement, as required by applicable state and federal laws, rules, and regulations. Contractor agrees to maintain said licenses, permits, and certificates in good standing for the duration of this Agreement. A copy of each such licenses, permits, and certificates shall be made available upon request, not to exceed three (3) business days after the initial request, for inspection, review, and/or audit by authorized representatives and designees of County, state, and/or federal governments during the term of this Agreement and for the applicable records retention period. Failure to maintain said licenses, permits, and/or certificates in effect for the duration of this Agreement shall be deemed a material breach of this Agreement and constitutes grounds for immediate termination of this Agreement by County. Staff shall only function within the scope of practice as dictated by licensing boards/bodies. At all times during the term of this Agreement, Contractor shall have available and shall provide upon request to authorized representatives of County a list of all persons by name, title, professional degree, and experience who are providing any services under this Agreement.

10.21. Charitable Choice/Faith-Based Organizations

Contractor agrees and acknowledges that County may make funds available for programs or services affiliated with religious organizations under the following conditions: (i) the funds are made available on an equal basis for programs or services affiliated with non-religious organizations; (ii) the program funded does not have the substantial effect of supporting religious activities; (iii) the funding is indirect, remote, or incidental to the religious purpose of the organization.

10.21.1. Contractor agrees and acknowledges that County may not make funds available for programs or services affiliated with a religious organization that (i) has denied or continues to

deny access to services on the basis of race, color, religion, ancestry, national origin, sex, citizenship, or known disability; (ii) will use the funds for a religious purpose; (iii) will use the funds for a program or service that subjects its participants to religious education.

10.21.2. Contractor agrees and acknowledges that all recipients of funding from County must (i) comply with all legal requirements and restrictions imposed upon government-funded activities set forth in Article IX, Section 8 and Article XVI, Section 5 of the California Constitution and in the First Amendment to the United States Constitution; and (ii) segregate such funding from all funding used for religious purposes.

#### 11. Demand for Assurance

Each party to this Agreement undertakes the obligation that the other party's expectation of receiving due performance will not be impaired. When reasonable grounds for insecurity arise with respect to the performance of either party, the other party may in writing demand adequate assurance of due performance, and until such assurance is received may, if commercially reasonable, suspend any performance for which the agreed return has not been received. "Commercially reasonable" includes not only the conduct of a party with respect to performance under this Agreement, but also conduct with respect to other agreements with parties to this Agreement or others. After receipt of a justified demand, failure to provide within a reasonable time, but not exceeding 30 days, such assurance of due performance as is adequate under the circumstances of the particular case is a repudiation of this Agreement. Acceptance of any improper delivery, service, or payment does not prejudice the aggrieved party's right to demand adequate assurance of future performance. Nothing in this Article limits County's right to terminate this Agreement pursuant to Article 4 (Termination).

#### 12. Assignment and Delegation

Neither party hereto shall assign, delegate, sublet, or transfer any interest in or duty under this Agreement without the prior written consent of the other party, and no such transfer shall be of any force or effect whatsoever unless and until the other party shall have so consented.

#### 13. Method and Place of Giving Notice, Submitting Bills, and Making Payments

All notices, bills, and payments shall be made in writing and shall be given by personal delivery or by U.S. Mail or courier service. Notices, bills, and payments shall be addressed as follows:

To County:	To Contractor:
Ken Tasseff Healthcare Privacy and Security Officer Sonoma County Department of Health Services 1450 Neotomas Avenue, Suite 200 Santa Rosa, CA 95405 Phone: (707) 565-4703 Email: ken.tasseff@sonoma-county.org	Jim Brahm Chief Executive Officer Security Compliance Associates 2727 Ulmerton Road, Suite 310 Clearwater, FL 33762 Phone: (727) 571-1141 Email: BrianF@scasecurity.com

When a notice, bill, or payment is given by a generally recognized overnight courier service, the notice, bill, or payment shall be deemed received on the next business day. When a copy of a notice, bill, or payment is sent by facsimile or email, the notice, bill, or payment shall be deemed received upon transmission as long as: (1) the original copy of the notice, bill, or payment is

promptly deposited in the U.S. Mail and postmarked on the date of the facsimile or email (for a payment, on or before the due date); (2) the sender has a written confirmation of the facsimile transmission or email; and (3) the facsimile or email is transmitted before 5 p.m. (recipient's time). In all other instances, notices, bills, and payments shall be effective upon receipt by the recipient. Changes may be made in the names and addresses of the person to whom notices are to be given by giving notice pursuant to this Article 13.

#### 14. Miscellaneous Provisions

##### 14.1. No Waiver of Breach

The waiver by County of any breach of any term or promise contained in this Agreement shall not be deemed to be a waiver of such term or provision or any subsequent breach of the same or any other term or promise contained in this Agreement.

##### 14.2. Construction

To the fullest extent allowed by law, the provisions of this Agreement shall be construed and given effect in a manner that avoids any violation of statute, ordinance, regulation, or law. The parties covenant and agree that in the event that any provision of this Agreement is held by a court of competent jurisdiction to be invalid, void, or unenforceable, the remainder of the provisions hereof shall remain in full force and effect and shall in no way be affected, impaired, or invalidated thereby. Contractor and County acknowledge that they have each contributed to the making of this Agreement and that, in the event of a dispute over the interpretation of this Agreement, the language of the Agreement will not be construed against one party in favor of the other party. Contractor and County acknowledge that they have each had an adequate opportunity to consult with counsel in the negotiation and preparation of this Agreement.

##### 14.3. Consent

Wherever in this Agreement the consent or approval of one party is required to an act of the other party, such consent or approval shall not be unreasonably withheld or delayed.

##### 14.4. No Third-Party Beneficiaries

Nothing contained in this Agreement shall be construed to create and the parties do not intend to create any rights in third parties.

##### 14.5. Applicable Law and Forum

This Agreement shall be construed and interpreted according to the substantive law of California, regardless of the law of conflicts to the contrary in any jurisdiction. Any action to enforce the terms of this Agreement or for the breach thereof shall be brought and tried in the City of Santa Rosa or the forum nearest to the City of Santa Rosa in the County of Sonoma.

##### 14.6. Captions

The captions in this Agreement are solely for convenience of reference. They are not a part of this Agreement and shall have no effect on its construction or interpretation.

##### 14.7. Merger

This writing is intended both as the final expression of the Agreement between the parties hereto with respect to the included terms and as a complete and exclusive statement of the terms of the Agreement, pursuant to Code of Civil Procedure Section 1856. Each party acknowledges

that, in entering into this Agreement, it has not relied on any representation or undertaking, whether oral or in writing, other than those which are expressly set forth in this Agreement. No modification of this Agreement shall be effective unless and until such modification is evidenced by a writing signed by both parties.

14.8. Survival of Terms

All express representations, waivers, indemnifications, and limitations of liability included in this Agreement will survive its completion or termination for any reason.

14.9. Time of Essence

Time is and shall be of the essence of this Agreement and every provision hereof.

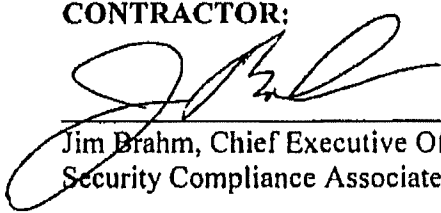
14.10. Counterparts and Electronic Copies

The parties agree that, where applicable, this Agreement may be executed in counterparts, together which when executed by the requisite parties shall be deemed to be a complete original agreement. An electronic copy, including facsimile copy, email, or scanned copy of the executed Agreement or counterpart, shall be deemed, and shall have the same legal force and effect as, an original document.

§ The remainder of this page has intentionally been left blank. §

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the Effective Date.

**CONTRACTOR:**

  
\_\_\_\_\_  
Jim Brahm, Chief Executive Officer  
Security Compliance Associates

7/26/19  
\_\_\_\_\_  
Dated

**COUNTY OF SONOMA:**

Certificate of Insurance on File with County:

\_\_\_\_\_  
Barbie Robinson, Director  
Department of Health Services

\_\_\_\_\_  
Dated

Approved as to Substance:

\_\_\_\_\_  
Division Director or Designee

\_\_\_\_\_  
Dated

Approved as to Form:

  
\_\_\_\_\_  
Sonoma County Counsel

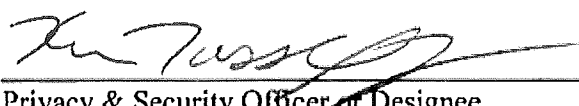
8/1/19  
\_\_\_\_\_  
Dated

Approved as to Substance:

\_\_\_\_\_  
Information Systems Manager

\_\_\_\_\_  
Dated

Approved as to Substance:

  
\_\_\_\_\_  
Privacy & Security Officer or Designee

7/26/19  
\_\_\_\_\_  
Dated



**Exhibit A. Scope of Work and Budget****County of Sonoma RFP Scope of Services Sought**

The County wishes to engage Security Compliance Associates (SCA) to provide a Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) Privacy and Security Risk Analysis for multiple County departments and perform other services as further described below.

Pursuant to 45 Code of Federal Regulations (CFR) section 164.105, the County has established itself as a hybrid entity and has designated the following five (5) County departments as covered components of the Covered Entity (CE):

- Department of Health Services – Public Health, Behavioral Health, and Administration
- Human Services Department - Multipurpose Senior Services Program and Home Community Based Alternatives Program. (Approximately 5 staff in each program)
- County Counsel
- Human Resources – Self-Funded Health Plan, FSA, Liability and Insurance Unit
- Information Services Department

In an effort to ensure/achieve compliance with HIPAA/HITECH across all portions of the CE, the County has endeavored to create standards and practices for implementation countywide. In furtherance of that effort, the County desires to contract with an entity/organization to complete a HIPAA/HITECH Security Risk Analysis that meets the requirements of 45 CFR section 164.308(a), for each CE department. While completion of a Security Risk Analysis is a required element of this request, proposals are also sought for the completion of a HIPAA Privacy Rule Gap Analysis and Physical Assessment, to be performed at the County's discretion.

Taken directly from County of Sonoma, Department of Health Services – Request for Proposals #19-001:

**5.1. HIPAA Risk Analysis (45 CFR §164.308(a)(1)(ii)(A))**

Proposer shall perform the following:

- a. Penetration Testing (i.e. blind and intelligent)
- b. Vulnerability Assessment
- c. Physical assessment of technical infrastructure
- d. A systematic and thorough identification and evaluation of the County's information assets (data, information systems, and information processing facilities) which create, receive, maintain, or transmit electronic ePHI
- e. Potential risks to those identified information assets (to include potential costs of privacy or security breaches and other information security threats), and associated with how the department collects, uses, manages, stores, maintains, discloses, and disposes of information
- f. Existing privacy and security measures and the effectiveness of those measures
- g. Potential gaps or deficiencies in maintenance, protection, and utilization of the information assets
- h. Internal/external networks (including penetration tests)
- i. Internet/intranet vulnerability test

- j. Internet, Extranet and Intranet applications
- k. Wireless networks, including, but not limited to, secure and guest Wi-Fi access points.
- l. Servers and data storage.
- m. Workstations and peripheral endpoints
- n. Firewall diagnostics
- o. Virtual Private Network and remote access infrastructure
- p. Mobile devices
- q. Denial of service tests
- r. Social engineering tests
- s. Security architecture and configuration review
- t. Other items identified by the Proposer as recommended or necessary for a Risk Analysis

5.2. HIPAA Security Rule Gap Analysis – Addresses compliance with:

- a. §164.306 General Requirements
- b. §164.308 Administrative Safeguards
- c. §164.310 Physical Safeguards
- d. §164.312 Technical Safeguards
- e. §164.316 Policies, Procedures and Documentation

5.3. Privacy Rule Gap Analysis – Addresses compliance with:

- a. §164.502: Uses and Disclosure of Protected Health Information: General Rules
- b. §164.504: Uses and Disclosures: Organizational Requirements
- c. §164.506: Uses and Disclosures to Carry Out Treatment, Payment, or Health Care Operations
- d. §164.508: Uses and Disclosures for Which an Authorization is Required
- e. §164.510: Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object
- f. §164.512: Uses and Disclosures for Which an Authorization or Opportunity to agree or Object is Not Required
- g. §164.514: Other Requirements Relating to Uses and Disclosures of Protected Health Information.
- h. §164.520: Notice of Privacy Practices for Protected Health Information
- i. §164.522: Rights to Request Privacy Protection for Protected Health Information
- j. §164.524: Access of Individuals to Protected Health Information
- k. §164.526: Amendment of Protected Health Information
- l. §164.528: Accounting of Disclosures of Protected Health Information
- m. §164.530: Administrative Requirements

5.4. HIPAA Physical Assessment and End User Security Awareness Assessment

- a. Site visits as determined by the participating department to evaluate and document physical security controls that are currently implemented;
- b. Other activities identified by Proposer as recommended or necessary for a physical assessment.
- c. End User Security Awareness Assessment

- Interviews with selected staff regarding common privacy and security related practices within and between departments to measure end user security awareness.
- A review of existing privacy and security policies and procedures at both the department and County level, including policies regarding: breach reporting and response; personnel; business associate agreements; physical, technical and administrative safeguards; oversight and monitoring; and, HIPAA complaints.
- A review and evaluation of department and County level HIPAA training.
- Other activities identified by Proposer as recommended or necessary for assessing end user security awareness.

### Summary of SCA Services

To satisfy the services sought in County RFP #19-001, Security Compliance Associates will deliver the following:

1. HIPAA Security Risk Analysis
2. Internal Systems Vulnerability Assessment and Analysis
3. Internal Systems Penetration Testing
4. Information Asset Assessment
5. External Systems Vulnerability Assessment and Analysis
6. External Systems Penetration Testing
7. DoS Susceptibility Assessment
8. Application Penetration Testing
9. Social Engineering
10. HIPAA Security Gap Analysis
11. HIPAA Privacy Assessment
12. HIPAA Physical Assessment and End User Security Awareness Assessment

### Scope of Services

Certain efficiencies will be gained in delivering the services requested because 1) there are shared security, privacy and confidentiality policies between the five departments identified, 2) some of the departments are smaller and represent lower risk, and 3) because Sonoma County ISD supports multiple departments.

Department	Employees	Locations	Security P&P	Privacy P&P
Department of Health Services	650	12	DHS	DHS
Human Services Department	20	1	ISD ESP	DHS
County Counsel	8	1	ISD ESP	CC CP
Human Resources	5	1	ISD ESP	DHS
Information Services Department	60	3	ISD ESP	ISD CP

Referencing DHS RFP Section 5: Scope of Services:

Sections: 5.1 HIPAA Security Risk Analysis

5.2 HIPAA Security Rule Gap Analysis

5.4 HIPAA Physical Assessment and End User Security Awareness Assessment

SCA will conduct all requirements over one-week (five-day) period, on-site in Santa Rosa, CA. A team consisting of one (1) Senior Analyst and one (1) Junior Analyst will be sent to accommodate the scope of this portion of the engagement.

Section 5.1 HIPAA Security Risk Analysis – Items (d)(e)(g)

SCA will conduct all requirements over one-week (five-day) period, on-site in Santa Rosa, CA. A separate Senior Analyst will be sent to accommodate the scope of this portion of the engagement.

Section 5.3 HIPAA Privacy Rule

SCA will conduct all requirements over one-week (five-day) period, on-site in Santa Rosa, CA. The SVP of Compliance Services will personally accommodate the scope of this portion of the engagement.

External Vulnerability Assessment

External and Internal Penetration Testing

Application Penetration Testing

SCA will conduct all requirements remotely by a separate team of analysts led by the SCA Director of Cybersecurity Services.

Sonoma County DHS IT, ISD and/or information security personnel will be permitted to observe SCA during the assessments. High-level details/targets of Sonoma County DHS and participating department's environment for this engagement include:

Item	ISD	HSD
Physical Servers:	69	35
Virtualized Servers	689	150
Network Nodes	9000	2500
Network Switches or Routers	300	45
Wireless Access Points	225	64
Appliance based Firewalls	20	2
External Facing Live IP's	175	38
Number of Desktops By OS:		
Windows 10, Vista, 7 or 8	3000	1500
Windows XP	5	
Mac OS	5	
Number of Tablets:		
IOS	200	15
Android	80	
Windows	200	5

Internal IPs in-scope for Internal Vulnerability Assessment and Pen Test: ~24

(SCA assumes this is a range)

External IPs in-scope for Internal Vulnerability Assessment and Pen Test: ~12

Wireless network in-scope for testing: 1 SSID, 1 location

Internet, Extranet and Intranet Applications for Penetration Testing: 6

Main Location: 10 Charles Street, Providence, RI 02904

Social Engineering E-mail Phishing: 11 HSD employees up to overall preference

Social Engineering In-Person: Two locations

Physical Security: Six locations

### **HIPAA Security Risk Analysis**

The HIPAA Security Risk Analysis includes an analysis of the IT systems, controls, policies and procedures that affect the Confidentiality, Integrity and Availability of Sonoma County DHS and participating department IT systems and data. Security risks must be constantly evaluated against compliance and privacy needs. Since the County handles patient healthcare records and other private information, it is required to comply with multiple state, federal, and industry regulations and applicable laws such as:

<b>Enforcement</b>	<b>Applicable Regulatory Requirements &amp; Laws</b>	<b>Potential Organizational Impact</b>
Office of Civil Rights	<ul style="list-style-type: none"> <li>• 45 CFR 164.306</li> <li>• 45 CFR 164.308</li> <li>• 45 CFR 164.310</li> <li>• 45 CFR 164.312</li> <li>• 45 CFR 164.314</li> <li>• 45 CFR 164.316</li> <li>• 45 CFR 164.400 – 414</li> </ul>	<ul style="list-style-type: none"> <li>• Establishes a requirement for Administrative, Technical and Physical safeguards in compliance with HIPAA and HITECH.</li> </ul>
California Dept of Technology	<ul style="list-style-type: none"> <li>• SIMM 5340-C</li> </ul>	<ul style="list-style-type: none"> <li>• Requirements for notification following a breach</li> <li>• Requirements to respond to incidents involving a breach</li> </ul>

The results of this assessment are specifically intended to assist management with making rational and well-supported risk-based decisions concerning the information system security controls. SCA will align the findings with HIPAA-focused Administrative, Technical and Physical categories, which further aids management in the identification and understanding of findings and remediation.

The HIPAA Security Risk Analysis report represents a snapshot in time on the security posture of Sonoma County DHS and participating departments. In order to satisfy HIPAA requirements, SCA will provide:

- Security Risk Remediation Report, which covers the People and Process related risks to Electronic Protected Health Information (ePHI),
- Technical Vulnerability Assessment Report, which covers the Information Technology (IT) related risks to ePHI.

Following the assessment, you will be presented the most significant findings of the Risk Analysis. The significance is based in part on whether the control is required or addressable by the Health Insurance Portability and Accountability Act (HIPAA). Within the context of this assessment, SCA will apply a 'Best Practices' overlay to the engagement.

The process developed by Security Compliance Associates for conducting the HIPAA Security Risk Analysis is as follows:

- 1. Conduct a Risk Analysis using SCA proprietary methodology** - as depicted in Figure 1 below incorporating NIST 800-30 Rev. 1 (Guide for Conducting Risk Assessments), NIST 800-66 (Implementing the HIPAA Security Rule) and the risk analysis spreadsheet developed by the Office of the National Coordinator's HealthIT.gov staff, which was modified and enhanced by SCA. The spreadsheet covers Risk Analysis of people, processes and procedures within the organization.

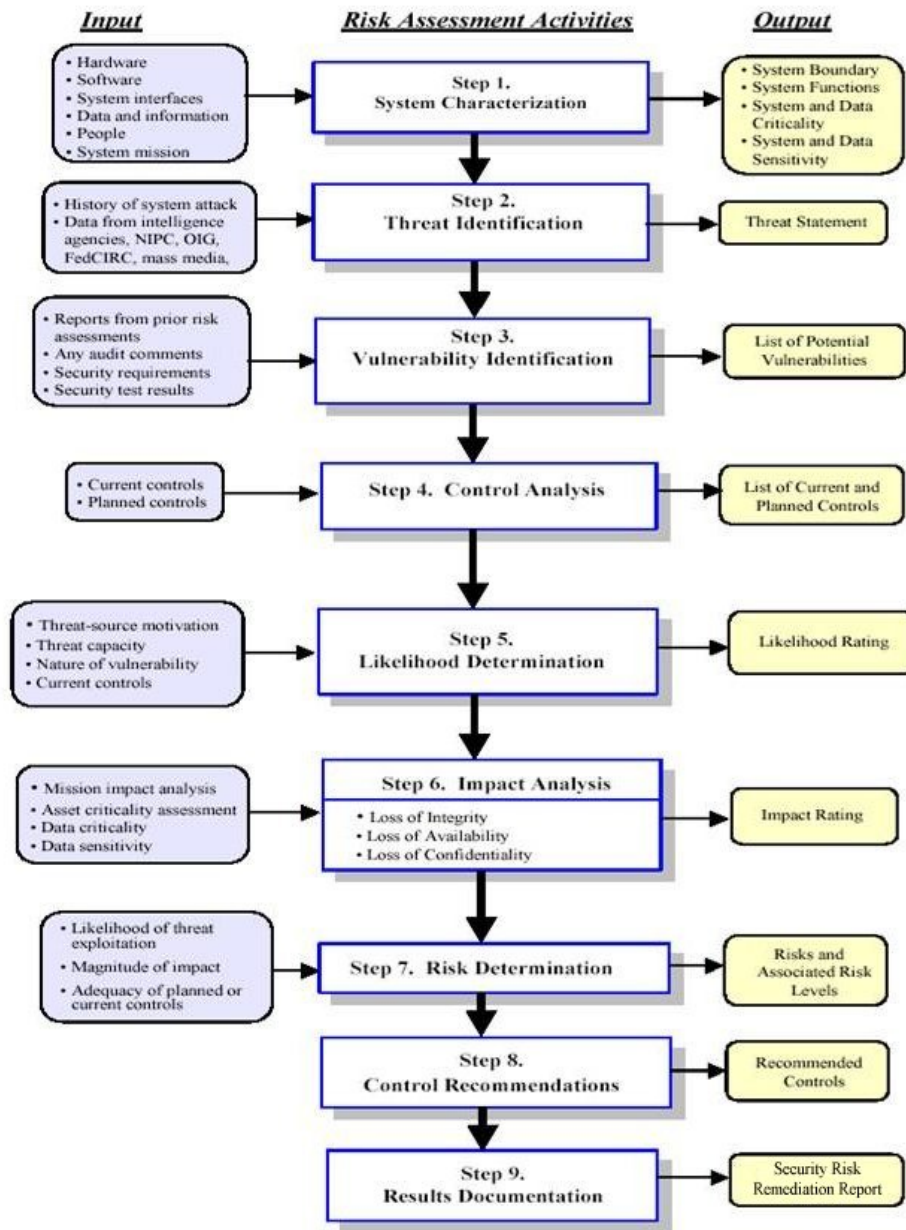


Figure 1 SCA's Risk Analysis Methodology (adapted from NIST SP 800-30)

## **HIPAA Security Risk Analysis Process:**

### Preparing for the Assessment

This step establishes the context for the risk analysis. SCA will work with Sonoma County DHS to identify the requirements for conducting the risk analysis, specific assessment methodologies to be employed, procedures for selecting risk factors that should be considered, the scope of the assessments, rigor of analyses, degree of formality, and requirements that facilitate consistent and repeatable risk determinations across the practice's information systems.

The HIPAA Security Risk Analysis begins with the identification of assets and resources including printed, stored, and electronic information/media, information system components including hardware, software, and operating environment on all interfaces, and interconnections associated with systems identified in the scope of the assessment.

### Conducting the Analysis

A list of information security threats/vulnerabilities that can be prioritized by risk level and used to inform risk response decisions is created. SCA will analyze the threats and vulnerabilities, impacts and likelihood of harm, and the uncertainty associated with the risk analysis process. SCA will gather essential information as a part of each task to assure that this step is conducted in accordance with the assessment context established in the previous step. The objective is to adequately cover the entire threat environment in accordance with the specific definitions, guidance, and direction established during the first step. The following techniques are used in gathering information:

- **On-site Interviews:** Interviews with practice support and management personnel enable risk assessment personnel to collect useful information about the system (e.g., how the system is operated and managed). On-site visits also allow risk assessment personnel to observe and gather information about the physical, environmental, and operational security of the IT system.
- **Document Review:** Policy documents, system documentation (e.g., system user guide, system administrative manual, system design and requirement document, acquisition document), and security-related documentation (e.g., previous audit report, risk assessment report, system test results, system security plans, security policies) will be used to gather information about the security controls used by and planned for the IT system.
- **Use of Automated/Manual Scanning Tools:** For network devices, tools will be used to identify the services that are currently running on a large group of hosts and provide a quick way of building individual profiles of the target system(s).

### Threat Identification

A threat is the potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability. Threat-sources are any circumstances or events with the potential to cause harm to the practice, be they natural, human, or environmental. Threat actions are the mechanisms by which each identified threat source can harm or damage the practice by affecting the practice's information systems. A threat-source does not present a risk when there is no vulnerability that can be exercised.



### Analysis Results

This step communicates and documents the analysis results and promotes the sharing of risk-related information. The results help to ensure that management has the appropriate risk-related information needed to inform and guide their risk decisions. Risks to system security are identified and the probability of occurrence is determined. The objectives are to evaluate all vulnerabilities identified for the system(s) during the risk assessment and to consider potential and likely threats capable of exploiting those vulnerabilities. The determination of risk for a particular threat/vulnerability pair can be expressed as a function of:

- The likelihood of a given threat-source attempting to exercise a given vulnerability.
- The magnitude of the impact should a threat-source successfully exercise the vulnerability.
- The adequacy of planned or existing security controls for reducing or eliminating risk.

### Countermeasures and Maintaining

The last step will help identify and document existing controls and safeguards to help reduce the level of risk to the practice. Next, additional safeguards that would mitigate this impact are identified. The goal of this step is to assess the countermeasures being implemented and/or planned to mitigate the risks, and to recommend additional countermeasures to adequately alleviate the risks. As a result, Sonoma County DHS will have an accurate knowledge of their risk situation.

Specific areas reviewed for Sonoma County DHS include but are not limited to:

- **Media Security** – protection of all forms of physical storage media including paper documents
- **Hardware Security** – hardware maintenance and change controls, anti-theft, anti-tampering
- **Software Security** – software maintenance and change controls, software integrity, software copyright/licensing compliance, privileged program controls, anti-virus and related malicious software safeguards, database security, security design on new systems, risk management process
- **Network Security** – network device security, communications security, network access controls, Internet/Web security, intrusion detection, vulnerability testing, network change controls, firewalls & proxy servers, dialup access security, encryption, e-mail security
- **Host (System) Security** – multi-user and single-user (workstation) computer operating system access controls including user authentication, data access authorization, audit logs; application security
- **Procedural Security** – information security charter, policies and procedures, organization, roles & responsibilities, auditing, awareness, IT change controls
- **Personnel Security** – background checks, non-disclosure agreements, training, professional development, terminations & transfers, contracts
- **Disaster Recovery/Business Continuity Planning** – Fault tolerance/redundancy, data backup, recovery/continuity planning
- **Physical Security** – facilities access control, security cameras, location and appropriate labeling of facilities access points, exits, facilities, etc.

- **Environmental Security** – disaster/interruption avoidance, safety, air conditioning and temperature controls, electrical power and utilities
- **Contractual Security/Privacy** – Business Associate Agreements, non-disclosure-agreements

**2. Perform network vulnerability testing** - Using state-of-the-art commercially available vulnerability assessment utilities, SCA will perform a technical vulnerability assessment of Sonoma County DHS's Internal and External systems. This is accomplished in three distinct phases as follows:

- **Discovery**

The discovery phase of the assessment process begins with a user-defined network element discovery and verification scan. During this process, the network is scanned for devices to confirm that the actual hosts and infrastructure components on the County's network are in place and active.

- **Testing**

The Testing phase of the process involves analyzing the configuration of specific hosts for known vulnerabilities associated with applications, operating systems configuration parameters and other security related attributes. Utilizing the data gathered during the Discovery Phase, a SCA analyst will analyze raw data for each host running in the client's address space. This data includes technical configuration elements including the current version of the operating systems, active ports, potential vulnerabilities, services and other configuration information.

- **Data Assembly**

The findings associated with the County's host analysis are entered into a secure database where the results for each host are maintained. The raw data from the Discovery and Testing phases is reviewed by SCA analysts to help alleviate any suspected "false positives." This final data is then compiled into a "findings matrix" that details and categorizes the vulnerabilities by individual host.

Please see the Internal and External Vulnerability Assessment sections below for more details.

**3. Facility Walkthrough – Physical Security Review** – An onsite walkthrough of DHS facilities is conducted to perform an analysis of the following areas:

- Administration: identification, courier/messenger services, janitorial services and access control.
- External Conditions: exterior doors, windows, roof access, lighting and air ducts.
- Physical Protections: keys, anti-theft devices and physical location of devices.
- Emergency Systems: emergency power and water shut off as well as emergency lighting.
- Vital Records: server room, media storage and protection.

Per the Sonoma County DHS RFP, six (6) locations are in-scope for Physical Security.

**4. Report Compilation** – The risk ratings and control recommendations are used to create the Security Risk Remediation Report. Threats are listed with likelihood of occurrence, impact rating and resulting risk rating along with risk remediation recommendations. It also has

columns for the County to assign the task to a staff member or vendor, along with a date for completion. The HIPAA Security Risk Analysis reporting is segmented and presented as follows:

- Table of Contents
- Purpose
- Approach – Tasks, Techniques and Rating Scale
- Threat Identification
- Results
- Plan of Action and Milestones
  - Threats/Impact Description
  - Vulnerabilities
  - Threat Source/Agent
  - Recommendations
  - Threat Probability
  - Impact Risk Rating
  - Risk Rating
  - Resources Required
  - Completion Date
  - Accepted Risk Date
  - Residual Risk

#### **Vulnerability Severity and Risk Level Matrices:**

Likelihood, impact, and the resulting risk ratings are qualitative assessments that utilize aspects of the NIST Guide for Conducting Risk Assessments (as shown in the following tables) and the information security assessor's professional experience and training. The following risk level scales are used in conjunction with the previously mentioned sources to most effectively determine a qualitative rating appropriate to the institution and the risk factor being evaluated.

**Likelihood** (Based on the NIST SP 800-30 Rev.1, Guide for Conducting Risk Assessments definitions for Risk and Information Security Risk, Table G-3 Assessment Scale – Likelihood of Threat Event Occurrence (Non-Adversarial))

<b>Value</b>	<b>Description</b>
High	Action is highly likely to occur.
Medium	Action is somewhat likely to occur.
Low	Action is unlikely to occur

**Impact** (Based on the NIST SP 800-30 Rev.1, Guide for Conducting Risk Assessments definitions for Risk and Information Security Risk, Table H-3 Assessment Scale – Impact of Threat Events)

<b>Value</b>	<b>Description</b>
High	Expected to have <b>severe or catastrophic</b> adverse effects on protected information and/or cause a <b>high</b> degree of regulatory criticism
Medium	Expected to have <b>serious</b> adverse effects on protected information and/or cause a <b>moderate</b> degree of regulatory criticism

Value	Description
Low	Expected to have <b>limited or negligible</b> adverse effects on protected information and/or cause a <b>low</b> degree or <b>no</b> regulatory criticism

**Risk** (Based on the NIST SP 800-30 Rev.1, Guide for Conducting Risk Assessments definitions for Risk and Information Security Risk, Table I-2 Assessment Scale – Level of Risk)

Likelihood	Impact		
	Low	Medium	High
High	Low	Medium	High
Medium	Low	Medium	Medium
Low	Low	Low	Low

### Internal Systems Vulnerability Assessment and Analysis

The Internal Systems Vulnerability Assessment and Analysis (ISVAA) is designed to assess the security posture of Sonoma County DHS and participating department internal network and systems. Active devices on the network are evaluated. The information security analysts will examine your internal information systems for implementation of industry best practices and perform a technical review to identify and report known vulnerabilities and configuration errors. SCA will provide specific remediation advice, in plain English.

SCA's staff will leverage a combination of commercially licensed tools, alongside the power and popularity of open source tools to perform the assessment. Open Source tools are utilized because they are the "Tools of the Trade." An attacker may not elect to spend thousands of dollars on commercial tools when there are thousands of open source tools available that can provide the same, if not better, results. SCA licenses many software tools to compliment the assessment, providing a much deeper assessment than traditional open source tools used as a standalone benchmark.

Testing will be conducted with knowledge of the information systems. This will allow SCA to perform a thorough assessment to ensure that your systems meet industry best practices and conform to the required regulations. SCA will work directly with the IT staff to identify daily procedures. Network diagrams and configuration files will be reviewed in this phase. The ISVAA will include detailed reports that prioritize the findings as well as an assessment of the overall security posture.

Below is a high-level overview of the tasks that SCA will perform during the engagement:

- Network Discovery
- Review of Network and Systems
- Port Scanning
- Firewall and Router Configuration Reviews
- Manual Probing of Available Services
- Server Assessment
- Virtual Infrastructure Security Assessment
- Vulnerability Scanning
- Manual Review of Discovered Vulnerabilities
- User/Group Management Review

- Password Management Review
- Review of Information Systems Physical Access Controls
- Review of Server Auditing and Logging
- VoIP Assessment
- Review Anti-Virus Configuration
- Review Change Configuration Management Procedures
- Wireless Network Assessment
- Patch Management Review
- Log Management Review
- Server Assessment

During this process, SCA will assess Sonoma County DHS's technology infrastructure. SCA will review network configurations, ensuring that the environment is soundly fabricated and that proper IT security controls are instituted for both hardware and software. SCA will conduct a series of interviews with designated employees to document your current IT security posture. The following is a detail of several of the tasks that will be performed, as applicable:

### **Server Assessment**

During the Server Assessment, SCA will evaluate the security of Sonoma County DHS's critical servers by analyzing the operating system and application level security issues. SCA will check administrative and technical controls, identify potential and actual weaknesses and recommend specific countermeasures.

SCA will check for the latest security patches and configuration methods for the latest applications. SCA will assess the following key areas during the Server Assessment:

- **Account management and security**
  - Password storage and restrictions
  - Password generation and management controls
  - User accounts permissions
  - Uniqueness of the accounts
  - Identify domain and sever account policies for password rules, login time restrictions and intruder detection and lockout
  - Test password policy
- **File Management and Security**
  - User permissions
  - File integrity
  - Antivirus software configuration and updates
  - Separation of privileges
- **Network Security**
  - Only necessary protocols are enabled
  - Only necessary services are running
  - Ensure that FTP, HTTP, NFS services have been secured (no anonymous or default configurations)
  - Host level firewall configuration check

- **Logging and Auditing**
  - Sufficient space is allocated for the logs
  - Logs are periodically reviewed
  - System times are in sync with the central server
- **Patch Level**
  - Pre-deployment patch testing environment
  - Security patches for operating systems have been applied
  - Security patches for applications have been applied
- **Detection of Previous Intrusions**
  - Scan for presence of viruses and back doors
  - Check suspicious file permissions
  - Check suspicious user accounts
  - Physical security
  - Back-up strategy
  - UPS
  - Fire suppressions are up to code
  - Environment – such as AC, Humidity

### **Firewall and Router Assessment**

During the Firewall and Router Assessment, SCA will review boundary device configurations and architectures, perform vulnerability scans as needed and perform interviews with firewall/network administrators.

Network diagrams and interviews with network administrators are conducted so that SCA can fully understand your network and its vulnerabilities.

During the Firewall and Router Configuration Review, SCA will target high-level concepts by tracking specific points such as:

- Policy and procedures documentation
- Network diagrams and data flows
- Third party connections
- Filtering rules that blacklist or whitelist traffic
- Firewall rules management
- IDS/IPS location and alerting
- Process of monitoring alerts
- Access controls to administer devices
- Software updates
- Remediation recommendations

### **Virtual Infrastructure Security Assessment**

The Virtual Infrastructure Assessment will help Sonoma County DHS identify and mitigate the risk to your virtual infrastructure by reviewing the architecture and design, policies, processes and people. SCA will evaluate if your virtual infrastructure is compliant with industry best practices. SCA combines the best of internal and external vulnerability testing for completing the

assessment. Virtual Infrastructure Security Assessment methodology consists of the following steps:

- Architecture and Design Review – Assess the virtual infrastructure and security practices specifically focusing on separation of networks, hosts and virtual machines
- Virtual Infrastructure Configuration Review – Assessment of the sampled virtual machines to ensure that no insecure configurations are present
- Virtual Infrastructure Security Testing and Patch Level Assessment
- Policy and Procedure Analysis – Evaluate the current policies and procedures for virtual infrastructure against best practices.

### **Wireless Network Assessment**

The Wireless Network Assessment includes a review of the wireless technologies in place, their design, configuration and access controls. Administrators will be interviewed, and documentation will be reviewed. For this assessment, the following areas will be addressed:

- Policies and procedures
- Wireless architecture and design
- Encryption and authentication configuration
- Network segmentation for the different wireless uses
- Wireless access point locations, broadcasting, and signal strength
- Analyze security gaps
- Remediation recommendations

### **Internal Systems Penetration Testing**

Penetration testing subjects systems to real-world attacks in an attempt to gain system access or obtain sensitive information. Internal Systems Penetration Testing involves two main components, an Internal Vulnerability Assessment to identify systems and potential vulnerabilities, and an Attack Phase where attempts are made to exploit vulnerabilities. The Attack Phase can also be known as the Exploitation and Post-Exploitation Phase. Testing will be performed remotely by SCA's C|EH, OSCP certified expert via a device provided to Sonoma County DHS.

The Internal Vulnerability Assessments will form the foundation for penetration testing. During the vulnerability assessments, SCA will identify:

- Information about a target that is freely available
- What systems might contain vulnerabilities
- What systems might contain valuable information
- What defenses are (or are not) in place

While performing reconnaissance of targets in scope, SCA will search for available information using sources such as:

- Whois
- Public records
- Internet searches
- News groups



- Client website(s)
- Domain Name System records
- Any other publicly facing systems

Next, SCA will perform discovery and probing of targets in scope with the following technical activities:

- Port scanning
- OS fingerprinting
- Manual probing of available services
- IDS/IPS evasion and alerting testing
- Vulnerability testing
- Manual validation of discovered vulnerabilities
- Identifying misconfigurations

The attack phase includes attempts to exploit found vulnerabilities to gain system access and/or sensitive information. Various techniques will be used including but not limited to manual techniques and automated tools. SCA will take precaution against disruption including a pre-assessment call to clearly identify expectations, rules of engagement and the identification of systems to exclude from testing. During the pre-assessment call, the client also reserves the right to require approval of any attempted exploitation of systems/services prior to any attempts by SCA personnel. Any critical vulnerabilities are immediately brought to your attention, so they may be remediated.

Upon completion, SCA will summarize the penetration testing results for each vulnerability with any information exploited, potential disruptions that could be executed and any remediation or mitigation techniques suggested. Information in this analysis includes:

- Vulnerability exploits attempted
- Vulnerability exploits successfully executed
- Methodologies used in exploiting vulnerabilities

### **Information Asset Assessment**

To accomplish items 5.1(d)(e)(g) as requested in the Sonoma county DHS RFP, SCA will perform an Information Asset Assessment. Using a combination of discovery/scanning tools, data collected during vulnerability assessments and interviews with appropriate DHS staff, SCA will:

- Identify and evaluate the County's information assets (data, information systems, and information processing facilities) which create, receive, maintain, or transmit electronic ePHI.
- Identify potential risks to those identified information assets (to include potential costs of privacy or security breaches and other information security threats), and associated with how the department collects, uses, manages, stores, maintains, discloses, and disposes of information.
- Identify potential gaps or deficiencies in maintenance, protection, and utilization of the information assets.



## **External Systems Vulnerability Assessment and Analysis**

The External Systems Vulnerability Assessment and Analysis (ESVAA) is designed to assess the security posture of Sonoma County DHS and participating department external network and systems. SCA's engineers will examine the external information systems for implementation of industry best practices and perform a technical review to exploit known vulnerabilities and configuration errors.

SCA's staff will leverage a combination of commercially licensed tools, alongside the power and popularity of open source tools to perform the assessment. Open Source tools are utilized because they are the "Tools of the Trade". An attacker may not elect to spend thousands of dollars on commercial tools when there are thousands of open source tools available that can provide the same, if not better, results. SCA licenses many software tools to compliment the assessment, providing a much deeper assessment than traditional open source tools used as a standalone benchmark.

The ESVAA is conducted in two very distinct phases. The first phase is reconnaissance. SCA's engineers will utilize multiple search engines and research public databases to gather information about Sonoma County DHS and its systems. Port scanning will also be performed during this phase. SCA will identify available services and begin foot printing the systems. The reconnaissance phase is often overlooked by novice attackers. They choose instead to go directly to heavier testing. The skilled attacker will not bypass this phase. They understand that reconnaissance is a vital step in compromising a network. Information collected in this stage can help the attacker better understand the institution's network and systems. The more knowledge he or she has about the systems, the less chance they have of being detected.

The second phase is the assessment phase. SCA's engineers will examine the systems for known vulnerabilities and misconfigurations. Automated tools will be utilized to identify possible areas of concern. Manual hands on techniques will then be executed to evaluate exploitability. SCA will immediately notify the designated point of contact upon discovery of critical vulnerabilities.

Below is a high-level overview of the tasks that SCA will perform and evaluate during the engagement:

- Port scanning
- OS fingerprinting
- Manual probing of available services
- IDS\IPS evasion and alerting testing
- Vulnerability testing
- Manual validation of discovered vulnerabilities
- Firewall Integrity

To assist Sonoma County DHS in securing the information systems, the results will be evaluated, and false positives will be removed. This produces a useful report that can be used to resolve problems. SCA will never provide a report that has been auto generated by a tool. Those reports tend to be extremely long and full of false positives.

SCA performs extensive tests on **all** provided external addresses, whether in use or not. SCA will document that dormant IP Addresses are in fact not in use. The live addresses are focused on for testing.

## External Systems Penetration Testing

Penetration testing subjects systems to real-world attacks in an attempt to gain system access or obtain sensitive information. External Systems Penetration Testing involves two main components, an External Vulnerability Assessment to identify systems and potential vulnerabilities, and an Attack Phase where attempts are made to exploit vulnerabilities. The Attack Phase can also be known as the Exploitation and Post-Exploitation Phase.

The External Vulnerability Assessments we perform for Sonoma County DHS will form the foundation for penetration testing. During the vulnerability assessments, SCA will identify:

- Information about a target that is freely available
- What systems might contain vulnerabilities
- What systems might contain valuable information
- What defenses are (or are not) in place

While performing reconnaissance of targets in scope, SCA will search for available information using sources such as:

- Whois
- Public records
- Internet searches
- News groups
- Client website(s)
- Domain Name System records
- Any other publicly facing systems

Next, SCA performs discovery and probing of targets in scope with the following technical activities:

- Port scanning
- OS fingerprinting
- Manual probing of available services
- IDS/IPS evasion and alerting testing
- Vulnerability testing
- Manual validation of discovered vulnerabilities
- Identifying misconfigurations

The attack phase includes attempts to exploit found vulnerabilities to gain system access and/or sensitive information. Various techniques will be used including but not limited to manual techniques and automated tools. SCA will take precaution against disruption including a pre-assessment call to clearly identify expectations, rules of engagement and the identification of systems to exclude from testing. During the pre-assessment call, the client also reserves the right to require approval of any attempted exploitation of systems/services prior to any attempts by SCA personnel. Any critical vulnerabilities are immediately brought to your attention, so they may be remediated.

Upon completion, SCA will summarize the penetration testing results for each vulnerability with any information exploited, potential disruptions that could be executed and any remediation or mitigation techniques suggested. Information in this analysis includes:

- Vulnerability exploits attempted
- Vulnerability exploits successfully executed
- Methodologies used in exploiting vulnerabilities

### **Denial of Service (DoS) Susceptibility Assessment**

The Denial of Service (DoS) Susceptibility Assessment is designed to analyze the security posture of Sonoma County DHS and its vendors that support its critical services. Denial of Service (DoS) attacks are among one of the most disruptive and malicious activities passing over the internet. DoS attacks can overwhelm web servers and saturate DHS' connection to the internet resulting in the inability to maintain efficient communications and connectivity and can ultimately impact business operations.

A comprehensive DoS program, structured around protecting, detecting and reacting is required to address the complete lifecycle of DoS attacks by:

- Strengthening systems and networks against attacks
- Detecting attacks when they occur
- Reacting appropriately to counter current and future attack trends

Developing an effective DoS preventative program is a significant task and one that requires communications with third party vendors, particularly internet and telecommunications service providers, and critical third-party vendors prior to an incident occurring.

SCA engineers will examine the external and internal network for implementation of industry best practices and perform a technical review to exploit known vulnerabilities and configuration errors that could lead to a Denial of Service attack being successfully executed. SCA will not launch an actual DoS attack against DHS' network since such an attack could disrupt critical business functions.

SCA gathers information from DHS and its critical vendors to determine their susceptibility to these types of attacks. SCA will examine SSAE-18s or similar, security white papers, FAQs, and internet sources about previous attacks. SCA will interview DHS personnel and vendors.

SCA will examine network architecture and bandwidth to determine alternate pathways that might be used in response to DoS attacks. SCA will also search, using open source intelligence gathering techniques, for DoS information related to DHS and its vendors.

### **Application Penetration Testing**

#### **Six applications per RFP and Addendum 1**

Application penetration testing subjects applications to real-world attacks in an attempt to determine whether unauthorized access or other malicious activity is possible. Application penetration testing involves two main components, an Application Assessment to identify potential vulnerabilities, and an Attack Phase where attempts are made to exploit vulnerabilities. The Attack Phase can also be known as the Exploitation and Post-Exploitation Phase.

SCA provides numerous automated and manual checks for web application vulnerabilities and incorporates testing for items related to OWASP Top 10 guidance for assessing potential vulnerabilities in applications. Because there are continuously evolving threats and

vulnerabilities, the client should regularly assess application security. SCA's in-depth analysis will provide the baseline for on-going evaluations. Testing will include the following elements.

- OWASP Top 10
  - Injection (SQL, LDAP, Xpath Flaws)
  - Broken Authentication and Session Management
  - Cross-Site Scripting (XSS)
  - Broken Access Control
  - Security Misconfiguration
  - Sensitive Data Exposure
  - Insufficient Attack Protection
  - Cross-Site Forgery Request (CSFR)
  - Using Components with Known Vulnerabilities
  - Underprotected APIs
- Malicious File Execution
- Information leakage and improper error handling
- Insecure cryptographic storage
- Insecure communications/transport layer protection
- Failure to restrict URL access

Additionally, SCA assesses the application for known vulnerabilities by using a combination of commercially available tools and licensed software. SCA will test security aspects related to functionality, usability, interface and compatibility. Testing includes internal links and out-going links from the specific domain(s). SCA will test the forms on web pages, including field validations, default values, incorrect inputs and modification options. Cookie testing is necessary for evaluating the application security. SCA will also validate HTML syntax errors. Database will be assessed for integrity, consistency and retrieval functions. It is necessary to test the navigation usability for vulnerabilities. Interface assessment includes validation that interactions between servers are executed properly. Compatibility testing for operating systems, browsers, mobile functions and printing options are conducted. If requested, web application security assessments may include load testing and stress testing.

The attack phase includes attempts to exploit found vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Various techniques will be used including but not limited to manual techniques and automated tools. SCA will take precaution against disruption including a pre-assessment call to clearly identify expectations and the rules of engagement. During the pre-assessment call, the client also reserves the right to require approval of any attempted exploitation of systems/services prior to any attempts by SCA personnel. Any critical vulnerabilities are immediately brought to your attention, so they may be remediated.

Upon completion, SCA will summarize the application penetration testing results for each vulnerability with any information exploited, potential disruptions that could be executed and any remediation or mitigation techniques suggested. Information in this analysis includes:

- Vulnerability exploits attempted
- Vulnerability exploits successfully executed
- Methodologies used in exploiting vulnerabilities

### **Social Engineering E-Mail Phishing**

E-mail phishing is a method used by attackers to trick employees into sharing sensitive information. E-mail messages are sent to employees asking them to provide login credentials which an attacker can then use to gain system access through a legitimate user account. Other types of e-mail messages sent may ask the employee to open an attachment or click on a link, either of which can trigger the installation of malware to aid the attacker in gaining access. SCA will send e-mail messages to your employees in an effort to gain sensitive information or take actions such as clicking a link. The goals of email phishing are to test employee awareness and response. Full details from the e-mail phishing exercise will be provided and become an important component of employee information security awareness training.

Because of the efficiency of SCA's email phishing platform and process, SCA is not limiting the number of phishing targets for this exercise. Therefore, all employees or a sampling of employees may be included per Sonoma County DHS preferences.

Attempts to penetrate nonpublic areas of facilities during and after business hours, attempts to gain access to employees' desktop computers, attempts to gain access to sensitive documents and information stored on other media are combined with the Facility Walkthrough - Physical Security Review.

### **HIPAA Security Rule Gap Analysis**

The HIPAA Security Rule Gap Analysis is performed in conjunction with the Internal Vulnerability Assessments and Analysis in order to evaluate Sonoma County DHS and participating department compliance in respect to safeguarding PHI and ePHI per the HIPAA Security Rule. It entails a comprehensive review of the existing information security posture. In order to evaluate compliance, as well as provide informed opinion, it is necessary to review the entire enterprise from a safeguarding PHI and ePHI point of view. The HIPAA Security Gap Analysis provides a baseline for the current state of practice and it will be measured against industry best practices, regulatory HIPAA compliance and SCA best practices. The HIPAA Security Rule Gap Analysis evaluates compliance with:

- 164.306 General Requirements
- 164.308 Administrative Safeguards
- 164.310 Physical Safeguards
- 164.312 Technical Safeguards
- 164.316 Policies, Procedures and Documentation
  - (HIPAA) Information Security Policy
  - Business Continuity and Disaster Recovery Plan
  - Incident Response Plan
  - Business Associate/Vendor Management Program

### **HIPAA Privacy Assessment**

The Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) defines standards for the use and disclosure of Protected Health Information, or PHI, by Covered Entities and Business Associates. PHI is all individually identifiable health information held or transmitted by a Covered Entity or Business Associate in any form including electronic, paper or oral. For individuals, the Privacy Rule provides rights to understand and control how their health information is used.

The HIPAA Privacy Assessment is a thorough review of Sonoma County DHS's privacy policies, standards and procedures to maintain the privacy of PHI and meet the requirements of the HIPAA Privacy Rule. The results of this assessment are specifically intended to assist management with making rational, well-supported decisions concerning the privacy controls in place and the direction of the privacy program.

#### Conducting the Assessment

SCA follows the OCR audit protocol to evaluate compliance with the HIPAA Breach Notification Rule and HIPAA Privacy Rule requirements below and itemized in the Sonoma County DHS RFP:

- 164.502: Uses and Disclosure of Protected Health Information: General Rules
- 164.504: Uses and Disclosures: Organizational Requirements
- 164.506: Uses and Disclosures to Carry Out Treatment, Payment, or Health Care Operations
- 164.508: Uses and Disclosures for Which an Authorization is Required
- 164.510: Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object
- 164.512: Uses and Disclosures for Which an Authorization or Opportunity to agree or Object is Not Required
- 164.514: Other Requirements Relating to Uses and Disclosures of Protected Health Information.
- 164.520: Notice of Privacy Practices for Protected Health Information
- 164.522: Rights to Request Privacy Protection for Protected Health Information
- 164.524: Access of Individuals to Protected Health Information
- 164.526: Amendment of Protected Health Information
- 164.528: Accounting of Disclosures of Protected Health Information
- 164.530: Administrative Requirements

An inventory of privacy policies, standards and procedures is created. SCA will evaluate the existence and adequacy of each privacy control as it pertains to its respective Privacy Rule section and requirement. The objective is to adequately cover the entire privacy spectrum from both provider and regulatory perspectives. The following techniques are used conduct the assessment:

Type	Description
<b>Inquiry</b>	Inquired of appropriate personnel seeking relevant information or representation including, among other things: <ul style="list-style-type: none"> <li>• Knowledge and additional information regarding the policy or procedure; and</li> <li>• Corroborating evidence of the policy or procedure.</li> </ul>
<b>Inspection</b>	Inspected documents and records indicating performance of the controls/practices.
<b>Observation</b>	Observed the existence of specific controls as represented.
<b>Testing/Sampling</b>	Validation of control/practice to ensure the accuracy of its operation.

#### Analysis Results

The HIPAA Privacy Assessment report represents a snapshot in time on the privacy posture of Sonoma County DHS. To understand how Sonoma County DHS's privacy program aligns with



the HIPAA Privacy Rule, SCA will provide the HIPAA Privacy Assessment report which presents the following organized by HIPAA Privacy Rule Section:

- Key Activity
- Established Performance Criteria including the Standard, Definition(s) and Implementation Specifications
- Audit Inquiry
- Whether Required or Addressable
- SCA Findings
- SCA Recommendations

### **HIPAA Physical Assessment and End User Security Awareness Assessment**

The Sonoma County RFP requests the Physical Assessment and End User Security Awareness assessment be broken out for consideration against available and/or limited budget. While SCA is sensitive to this request, the HIPAA Security Rule requires an evaluation of Technical, Administrative and Physical Safeguards to protect both PHI and ePHI. Due to this regulatory requirement, Physical Assessment/Security and End User Security Awareness are part of the normal HIPAA Security Risk Analysis and Gap Analysis process and reported in these deliverables. If Sonoma County DHS would like a separate report specifically for Physical Assessment and End User Security Awareness, SCA will be happy to provide one upon request in the Project Planning stage.

Please refer to HIPAA Security Risk Analysis Process, Item 3, Facility Walkthrough – Physical Security Review and Social Engineering which address physical security. End User Security Awareness is evaluated during the email phishing exercise as well as with select employee interviews and observations against information security policy and procedure.

The guarantee of compliance is contingent upon SCA evaluation against all regulatory requirements and Sonoma DHS implementation of corrective advice.

Over the course of the on-site service delivery, SCA will visit the following locations as identified in the RFP:

Physical Security	Locations
Department of Health Services:	
<i>Neotomas Avenue, Administrative Complex</i>	1
<i>Challenger Way Behavioral Health Campus</i>	1
<i>Human Services (Westwind Blvd.)</i>	1
Downtown Public Health offices	1
HR (Administration Complex)	1
County Counsel (Administration Complex)	1

### **Deliverables**

SCA provides custom reports for each project phase. Separate reports will be generated for the following assessments/services:

1. HIPAA Security Risk Analysis

2. Internal Systems Vulnerability Assessment and Analysis
3. Internal Systems Penetration Testing
4. Information Asset Assessment
5. External Systems Vulnerability Assessment and Analysis
6. External Systems Penetration Testing
7. DoS Susceptibility Assessment
8. Application Penetration Testing
9. Social Engineering
10. HIPAA Security Gap Analysis
11. HIPAA Privacy Assessment
12. HIPAA Physical Assessment and End User Security Awareness Assessment (Upon request as this is covered in HIPAA Security Risk Analysis and Gap Analysis)

The reports contain executive summaries and reflect individual sections, highlighting each unique assessment focus, and offer specific vulnerability findings, prioritization, recommendations and remediation advice. SCA allows for management comment columns, per request.

The reports are segmented and presented as follows:

- Table of Content
- Purpose
- Executive Summary-high level review of process, findings and ranking against known standards and/or peers.
- Vulnerability Classifications – identifies how each classification level, severe, high, medium, and low are defined.
- Approach and Methodology – explanation of various phases of the engagement.
- Assessment results- segmented by examined area
- Observations- with risk, background, and recommendations.
- Column for client response to findings

With the size and scope of this project, SCA anticipated draft reports are delivery in approximately 45 days from completion of testing. Sonoma County DHS will have the opportunity to review the report and findings with the SCA analyst team, add management comments and/or compensating logic before the final reports are issued.



**Sonoma County DHS Detailed and Annualized Pricing**

The Total Project Fees below reflect all project costs associated with the project.

<b>Description</b>	<b>Annual Qty.</b>	<b>Hours</b>	<b>Total</b>
<b>HIPAA Security Risk Analysis</b>	1	100	<b>\$19,000</b>
Internal Systems Vulnerability Assessment and Analysis	1	80	<b>\$15,200</b>
Internal Systems Penetration Testing	1	15	<b>\$3,300</b>
Information Asset Assessment	1	60	<b>\$11,400</b>
External Systems Vulnerability Assessment and Analysis	1	30	<b>\$5,700</b>
External Systems Penetration Testing	1	15	<b>\$3,300</b>
DoS Susceptibility Assessment	1	40	<b>\$7,600</b>
Application Penetration Testing	6	100	<b>\$22,000</b>
Social Engineering	1	20	<b>\$3,800</b>
<b>HIPAA Security Gap Analysis</b>	1	40	<b>\$7,600</b>
<b>HIPAA Privacy Assessment</b>	1	100	<b>\$19,000</b>
<b>HIPAA Physical Assessment and End User Security Awareness Assessment</b>	1	0	<b>\$0</b>
<b>Project Hours and Fees:</b>		600	<b>\$117,900</b>
Travel, Lodging and Meals	4		<b>\$7,200</b>
<b>Total Project Fees</b>			<b>\$125,100</b>
Hourly Fee for ongoing assessments or consulting	\$190		
Hourly Fee for ongoing penetration testing	\$220		

**Sonoma County DHS Proposed Project Invoicing**

Per the RFP, the County's policy is to not pay for services before it receives them, and per the Sample Professional Services Agreement, "Contractor shall be paid on a time-and-material/expense basis in accordance with the budget set forth in Exhibit B (Budget), attached hereto and incorporated herein by this reference (hereinafter "Exhibit B"). Following these guidelines, SCA proposes to invoice based on completion of each Project Stage as follows:

<b>Invoicing by Project Stage</b>	<b>Due Ending</b>	<b>Amount</b>
<b>Planning</b>	Week 3	<b>\$11,790</b>
<b>Discovery</b>	week 8	<b>\$47,160</b>
Travel, Lodging and Meals	Week 8	<b>\$7,200</b>
<b>Reporting</b>	Week 12	<b>\$47,160</b>
<b>Communication</b>	Week 16	<b>\$11,790</b>
<b>Total Project Fees</b>		<b>\$125,100</b>

**Exhibit B. Insurance Requirements**

(Template 5 – Ver. 01/09/18)

With respect to performance of work under this Agreement, Contractor shall maintain and shall require all of its subcontractors, consultants, and other agents to maintain insurance as described below unless such insurance has been expressly waived by the attachment of a *Waiver of Insurance Requirements*. Any requirement for insurance to be maintained after completion of the work shall survive this Agreement.

County reserves the right to review any and all of the required insurance policies and/or endorsements, but has no obligation to do so. Failure to demand evidence of full compliance with the insurance requirements set forth in this Agreement or failure to identify any insurance deficiency shall not relieve Contractor from, nor be construed or deemed a waiver of, its obligation to maintain the required insurance at all times during the performance of this Agreement.

**1. Workers Compensation and Employers Liability Insurance**

- a. Required if Contractor has employees as defined by the Labor Code of the State of California.
- b. Workers Compensation insurance with statutory limits as required by the Labor Code of the State of California.
- c. Employers Liability with minimum limits of \$1,000,000 per Accident; \$1,000,000 Disease per employee; \$1,000,000 Disease per policy.
- d. Required Evidence of Insurance: Certificate of Insurance.

If Contractor currently has no employees as defined by the Labor Code of the State of California, Contractor agrees to obtain the above-specified Workers Compensation and Employers Liability insurance should employees be engaged during the term of this Agreement or any extensions of the term.

**2. General Liability Insurance**

- a. Commercial General Liability Insurance on a standard occurrence form, no less broad than Insurance Services Office (ISO) form CG 00 01.
- b. Minimum Limits: \$1,000,000 per Occurrence; \$2,000,000 General Aggregate; \$2,000,000 Products/Completed Operations Aggregate. The required limits may be provided by a combination of General Liability Insurance and Commercial Excess or Commercial Umbrella Liability Insurance. If Contractor maintains higher limits than the specified minimum limits, County requires and shall be entitled to coverage for the higher limits maintained by Contractor.
- c. Any deductible or self-insured retention shall be shown on the Certificate of Insurance. If the deductible or self-insured retention exceeds \$25,000 it must be approved in advance by County. Contractor is responsible for any deductible or self-insured retention and shall fund it upon County's written request, regardless of whether Contractor has a claim against the insurance or is named as a party in any action involving the County.

- d. **“County of Sonoma, its Officers, Agents, and Employees”** shall be endorsed as additional insureds for liability arising out of operations by or on behalf of the Contractor in the performance of this Agreement.
  - e. The insurance provided to the additional insureds shall be primary to, and non-contributory with, any insurance or self-insurance program maintained by them.
  - f. The policy definition of “insured contract” shall include assumptions of liability arising out of both ongoing operations and the products-completed operations hazard (broad form contractual liability coverage including the “f” definition of insured contract in ISO form CG 00 01, or equivalent).
  - g. The policy shall cover inter-insured suits between the additional insureds and Contractor and include a “separation of insureds” or “severability” clause which treats each insured separately.
  - h. Required Evidence of Insurance:
    - i. Copy of the additional insured endorsement or policy language granting additional insured status; and
    - ii. Certificate of Insurance.
3. Automobile Liability Insurance
- a. Minimum Limit: \$1,000,000 combined single limit per accident. The required limits may be provided by a combination of Automobile Liability Insurance and Commercial Excess or Commercial Umbrella Liability Insurance.
  - b. Insurance shall cover all owned autos. If Contractor currently owns no autos, Contractor agrees to obtain such insurance should any autos be acquired during the term of this Agreement or any extensions of the term.
  - c. Insurance shall cover hired and non-owned autos.
  - d. Required Evidence of Insurance: Certificate of Insurance.
4. Professional Liability/Errors and Omissions Insurance
- a. Minimum Limits: \$1,000,000 per claim or per occurrence; \$1,000,000 annual aggregate.
  - b. Any deductible or self-insured retention shall be shown on the Certificate of Insurance. If the deductible or self-insured retention exceeds \$25,000 it must be approved in advance by County.
  - c. If Contractor’s services include: (1) programming, customization, or maintenance of software; or (2) access to individuals’ private, personally identifiable information, the insurance shall cover:
    - i. Breach of privacy; breach of data; programming errors, failure of work to meet contracted standards, and unauthorized access; and
    - ii. Claims against Contractor arising from the negligence of Contractor, Contractor’s employees and Contractor’s subcontractors.

- d. If the insurance is on a Claims-Made basis, the retroactive date shall be no later than the commencement of the work.
- e. Coverage applicable to the work performed under this Agreement shall be continued for two (2) years after completion of the work. Such continuation coverage may be provided by one of the following: (1) renewal of the existing policy; (2) an extended reporting period endorsement; or (3) replacement insurance with a retroactive date no later than the commencement of the work under this Agreement.
- f. Required Evidence of Insurance: Certificate of Insurance specifying the limits and the claims-made retroactive date.

5. Standards for Insurance Companies

Insurers, other than the California State Compensation Insurance Fund, shall have an A.M. Best's rating of at least A:VII.

6. Documentation

- a. The Certificate of Insurance must include the following reference: DHS Contract No. 2019-0163-A00.
- b. All required Evidence of Insurance shall be submitted prior to the execution of this Agreement. Contractor agrees to maintain current Evidence of Insurance on file with County for the entire term of this Agreement and any additional periods if specified in Sections 1 – 4 above.
- c. The name and address for Additional Insured endorsements and Certificates of Insurance is:  

**County of Sonoma, its Officers, Agents, and Employees**  
**Attn: DHS – Contract & Board Item Development Unit**  
**1450 Neotomas Avenue. Suite 200**  
**Santa Rosa CA 95405**  
**Email: DHS-Contracting@sonoma-county.org**
- d. Required Evidence of Insurance shall be submitted for any renewal or replacement of a policy that already exists, at least ten (10) days before expiration or other termination of the existing policy.
- e. Contractor shall provide immediate written notice if: (1) any of the required insurance policies is terminated; (2) the limits of any of the required policies are reduced; or (3) the deductible or self-insured retention is increased.
- f. Upon written request, certified copies of required insurance policies must be provided within thirty (30) days.

7. Policy Obligations

Contractor's indemnity and other obligations shall not be limited by the foregoing insurance requirements.

#### 8. Material Breach

If Contractor fails to maintain insurance which is required pursuant to this Agreement, it shall be deemed a material breach of this Agreement. County, at its sole option, may terminate this Agreement and obtain damages from Contractor resulting from said breach. Alternatively, County may purchase the required insurance, and without further notice to Contractor, County may deduct from sums due to Contractor any premium costs advanced by County for such insurance. These remedies shall be in addition to any other remedies available to County.

**Exhibit C**

**BUSINESS ASSOCIATE ADDENDUM  
TO THE  
AGREEMENT FOR SERVICES  
BETWEEN  
COUNTY OF SONOMA  
AND  
SECURITY COMPLIANCE ASSOCIATES  
(Revised 2018 Sep 11)**

This Business Associate Addendum (“Addendum”) supplements and is made a part of the services agreement (“Agreement”) by and between County of Sonoma (“County”) and Security Compliance Associates (“Business Associate”).

**RECITALS**

WHEREAS, County is a Hybrid Entity as defined under 45 Code of Federal Regulations (“CFR”) Section 164.103;

WHEREAS, Security Compliance Associates is a Business Associate as defined under 45 CFR Section 160.103;

WHEREAS, County wishes to disclose certain information to Business Associate pursuant to the terms of Addendum, some of which information may constitute Protected Health Information (“PHI”), including electronic Protected Health Information (“ePHI”);

WHEREAS, County and Business Associate intend to protect the privacy and provide for the security of PHI, including ePHI, disclosed to Business Associate pursuant to Addendum in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104 191 (“HIPAA”), regulations promulgated thereunder by the U.S. Department of Health and Human Services, and other applicable laws; and

WHEREAS, as part of the HIPAA Regulations, the Privacy Rule and Security Rule require County to enter into a contract containing specific requirements with Business Associate prior to the disclosure of PHI, including ePHI, as set forth in, but not limited to, 45 CFR Sections 164.502(e), 164.504(e), and 164.308(b)(1) and contained in Addendum.

NOW THEREFORE, in consideration of the mutual promises below and the exchange of information pursuant to Addendum, the parties agree as follows:

1. Definitions

Terms used, but not otherwise defined, in Addendum shall have the same meaning as those terms in the HIPAA Regulations as set forth at 45 CFR Sections 160.103, 164.304, and 164.501.

1.1. HIPAA Regulations

“HIPAA Regulations” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules as set forth at 45 CFR Part 160 and Part 164.

1.2. Breach

“Breach” shall mean the acquisition, access, use, or disclosure of PHI in a manner not permitted under 45 CFR Part 164 Subpart E and that compromises the security or privacy of PHI as defined at 45 CFR Section 164.402.

1.3. Business Associate

“Business Associate” shall have the same meaning as the term “Business Associate” as set forth at 45 CFR Section 160.103.

1.4. Covered Entity

“Covered Entity” shall have the meaning given to such term under the Privacy Rule and the Security Rule, including, but not limited to, 45 CFR Section 160.103. For purposes of this Addendum, this term is intended to mean the County of Sonoma.

1.5. Data Aggregation

“Data Aggregation” shall have the same meaning as the term “Data aggregation” as set forth at 45 CFR Section 164.501.

1.6. Designated Record Set

“Designated Record Set” shall have the same meaning as the term “designated record set” as set forth at 45 CFR Section 164.501.

1.7. Disclosure

“Disclosure” shall mean the release of, transfer of, provision of access to, or divulging in any manner information outside the entity holding the information in accordance with 45 CFR Section 160.103.

1.8. Health Care Operations

“Health Care Operations” shall have the same meaning as “Health care operations” as set forth at 45 CFR Section 164.501.

1.9. Individual

“Individual” shall have the same meaning as the term “Individual” as set forth at 45 CFR Section 164.501, except that the term “Individual” as used in this Addendum shall also include a person who qualifies as a personal representative in accordance with 45 CFR Section 164.502(g).

1.10. Minimum Necessary

“Minimum Necessary” shall mean the minimum amount of PHI necessary for the intended purpose, as set forth at 45 CFR Sections 164.502(b) and 164.514(d): Standard: Minimum Necessary.

1.11. Privacy Rule

“Privacy Rule” shall mean the HIPAA Standards for Privacy of Individually Identifiable Health Information as set forth at 45 CFR Part 160 and 45 CFR Part 164 Subparts A and E.

1.12. PHI

“PHI” shall have the same meaning as the term “protected health information” as set forth at 45 CFR Section 160.103, except limited to the information received from Covered Entity or created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity.

1.13. Required by Law

“Required by law” shall have the same meaning as the term “required by law” as set forth at 45 CFR Section 164.103.

1.14. Secretary

“Secretary” shall mean the Secretary of the United States Department of Health and Human Services (“DHHS”) or his/her designee.

1.15. Security Incident

“Security Incident” shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of personally identifiable information. A Security Incident includes the attempted or successful unauthorized access, use, disclosure, modification, or destruction of or interference with systems operations in an information system which processes PHI that is under the control of Covered Entity or Business Associate of Covered Entity, but does not include minor incidents that occur on a daily basis, such as scans, “pings”, or unsuccessful random attempts to penetrate computer networks or servers maintained by Business Associate.

1.16. Security Rule

“Security Rule” shall mean the HIPAA Security Standards for the Protection of ePHI as set forth at 45 CFR Part 160 and 45 CFR Part 164 Subparts A and E.

1.17. Subcontractor

“Subcontractor” shall mean a subcontractor of Business Associate that creates, receives, maintains, or transmits PHI on behalf of Business Associate.

1.18. Unsecured PHI

“Unsecured PHI” shall have the same meaning as the term “unsecured protected health information” as set forth at 45 CFR Section 164.402, except limited to the information received from Covered Entity or created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity.

1.19. Use

“Use” shall mean, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information in accordance with 45 CFR Section 160.103.

2. Obligations of Business Associate

Business Associate acknowledges that Business Associate is directly required to comply with the HIPAA Regulations and that Business Associate (including its subcontractors) may be held directly liable for and be subject to penalties for failure to comply. To the extent Business Associate is to carry out one or more of County's obligations under 45 CFR Part 164 Subpart E



---

of the Privacy Rule, Business Associate agrees to comply with the requirements of 45 CFR Part 164 Subpart E that apply to County in the performance of such obligations.

2.1. Use or Disclosure of Protected Health Information

Except as otherwise provided in Addendum, Business Associate shall use and/or disclose PHI only as necessary to perform functions, activities, or services documented in Exhibit A (Scope of Work and Budget) of Agreement for or on behalf of County, as specified in Addendum, provided that such use does not violate the HIPAA Regulations. Business Associate agrees not to further use or disclose PHI other than as permitted or required by Addendum or as required by law. Business Associate must make reasonable efforts to limit PHI to the Minimum Necessary to accomplish the intended purpose of the use, disclosure, or request. The uses of PHI may not exceed the limitations applicable to County under the HIPAA Regulations.

2.2. Safeguarding Protected Health Information

Business Associate shall use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for by Addendum. Business Associate shall implement administrative, physical, and technical safeguards and shall comply with 45 CFR Part 164 Subpart C with respect to ePHI that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI created, received, maintained, or transmitted on behalf of County and prevent the use or disclosure of PHI other than as provided for by Agreement.

- a. Encryption Requirements for Transmission and Storage of Electronic Data. All ePHI transmitted to Business Associate by County, and/or for or on behalf of County by Business Associate, and/or to County by Business Associate shall be provided or transmitted using encryption methods which renders such ePHI unusable, unreadable, or indecipherable by unauthorized persons. All ePHI stored by Business Associate on electronic media shall be protected using encryption methods which render such ePHI unusable, unreadable, or indecipherable by unauthorized persons. Encryption of ePHI in transit or at rest shall use a technology or methodology set forth by the Secretary in the guidance issued under Section 13402(h)(2) of Public Law 111-5, and in accordance with the National Institute of Standards Technology (NIST) and Standards and Federal Information Processing Standards (FIPS), as applicable.
- b. Destruction of PHI on paper, film, or other hard copy media must involve either shredding or otherwise destroying the PHI so that it cannot be read or reconstructed.
- c. Should any employee or subcontractor of Business Associate have direct, authorized access to County computer systems that contain ePHI, Business Associate shall immediately notify County of any change of such personnel (e.g., employee or subcontractor termination, or change in assignment where such access is no longer necessary) in order for County to disable the previously authorized access.

2.3. Notification of Breach, Unauthorized Use or Improper Disclosure

Business Associate must notify County in writing of any access, use, or disclosure of PHI not permitted or provided for by Addendum and/or any actual or suspected use or disclosure of

data in violation of any applicable federal or state laws or regulations of which Business Associate becomes aware. A breach or unauthorized access, use, or disclosure shall be treated as discovered by Business Associate the first day on which such unauthorized access, use, or disclosure is known, or should reasonably have been known, to Business Associate or to any person, other than the individual committing the unauthorized disclosure, that is an employee, officer, subcontractor, agent, or other representative of Business Associate.

- a. Notification must be made as soon as practicable, but not later than 24 hours after discovery, by telephone call to 707-565-5703 plus e-mail to: DHS-Privacy&Security@sonoma-county.org , and will include:
  1. The identification of each Individual whose PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used, or disclosed; and
  2. A description of any remedial action taken or proposed to be taken by Business Associate.
- b. Business Associate must mitigate any harm that results or may result from the breach, security incident, or unauthorized access, use, or disclosure of unsecured PHI by Business Associate or its employees, officers, subcontractors, agents, or other representatives.
- c. Following a breach or unauthorized access, use, or disclosure of unsecured PHI, Business Associate agrees to take any and all corrective action necessary to prevent recurrence, to document any such corrective action, and to make this documentation available to County.

#### 2.4. Agents and Subcontractors of Business Associate

In accordance with 45 CFR Sections 164.502(e)(1)(ii) and 164.308(b)(2), and to the extent that Business Associate uses any agent, including a subcontractor, to which Business Associate provides PHI received from, created by, maintained by, or received by Business Associate on behalf of County, Business Associate shall execute an agreement with such agent or contractor containing a requirement to ensure compliance with the same restrictions and conditions that apply through Addendum to Business Associate with respect to PHI.

#### 2.5. Access to Protected Health Information

At the request of County, and in the time and manner designated by County, Business Associate shall provide access to PHI in Designated Record Set to an Individual or County to meet the requirements of 45 CFR Section 164.524.

#### 2.6. Amendments to Designated Record Set

Business Associate shall make any amendment(s) to PHI in Designated Record Set as directed or agreed to by County, or to take other measures necessary to satisfy County's obligations under 45 CFR Section 164.526.

#### 2.7. Accounting of Disclosures

Business Associate shall document and make available such disclosures of PHI and information related to such disclosures as would be required for County to respond to a request

by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR Section 164.528.

2.8. Records Available to County, State, and Secretary

Business Associate shall make available internal practices, books, and records related to the use, disclosure, and privacy protection of PHI received from County, or created, maintained, or received by Business Associate on behalf of County, to County, State, or the Secretary for the purposes of investigating or auditing Business Associate's compliance with the HIPAA Regulations in the time and manner designated by County, State, or Secretary.

2.9. Return or Destruction of Protected Health Information

Upon termination of Addendum for any reason, Business Associate shall:

- a. (i) Return all PHI received from County; return all PHI created, maintained or received by Business Associate on behalf of County; and return all PHI required to be retained by the HIPAA Regulations; or (ii) at the discretion of County, destroy all PHI received from County, or created, maintained, or received by Business Associate on behalf of County. Destruction of PHI on paper, film, or other hard copy media must involve shredding or otherwise destroying the PHI in a manner which will render the PHI unreadable, undecipherable, or unable to be reconstructed. Business Associate shall certify in writing that such PHI has been destroyed.
- b. In the event Business Associate determines that returning or destroying PHI is not feasible, Business Associate shall provide County notification of the conditions that make return or destruction not feasible. Business Associate shall extend the protections of this Addendum to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

2.10. Data Aggregation

Business Associate may provide data aggregation services related to the health care operations of County as permitted by 45 CFR Section 164.504(e)(2)(i)(B).

2.11. Other Applicable Laws

Business Associate shall comply with all other applicable laws to the extent that such state confidentiality laws are not preempted by HIPAA.

2.12. Penalties/Fines for Failure to Comply with HIPAA

Business Associate shall pay any penalty or fine assessed against Covered Entity arising from Business Associate's failure to comply with the obligations imposed by HIPAA.

2.13. Training of Employees and Enforcement of Requirements

Business Associate shall train and use reasonable measures to ensure compliance with the requirements of this Business Associate Agreement by employees who assist in the performance of functions or activities on behalf of County under this Contract and use or disclose protected information; and discipline employees who intentionally violate any provisions.

### 3. Amendments to Addendum

No amendment of Addendum shall be effective unless and until such amendment is evidenced by a writing signed by the parties. County and Business Associate agree to take such action as is necessary to amend Addendum as required for County to comply with the requirements of the HIPAA Regulations. However, any provision required by HIPAA Regulations to be in Addendum shall bind the parties whether or not provided for in Addendum.

### 4. Termination of Addendum

If Business Associate should fail to perform any of its obligations hereunder, or materially breach any of the terms of Addendum, County may terminate Addendum immediately upon provision of notice stating the reason for such termination to Business Associate. County, within its sole discretion, may elect to give Business Associate an opportunity to cure such breach.

### 5. Material Breach

A breach by Business Associate or any of its agents or subcontractors of any provision of Addendum, as determined by County, shall constitute a material breach of Addendum and shall provide grounds for immediate termination of Addendum.

### 6. Indemnification

Business Associate agrees to accept all responsibility for loss or damage to any person or entity, including County, and to indemnify, hold harmless, and release County, its officers, agents, and employees from and against any actions, claims, damages, liabilities, disabilities, or expenses that may be asserted by any person or entity, including Business Associate, that arise out of, pertain to, or relate to Business Associate's or its agents', employees', contractors', subcontractors', or invitees' performance or obligations under Agreement. Business Associate agrees to provide a complete defense for any claim or action brought against County based upon a claim relating to such Business Associates' or its agents', employees', contractors', subcontractors', or invitees' performance or obligations under Agreement. Business Associates' obligations under Article 5 (Indemnification) apply whether or not there is concurrent negligence on County's part, but to the extent required by law, excluding liability due to County's conduct. County shall have the right to select its legal counsel at Business Associate's expense, subject to Business Associate's approval, which shall not be unreasonably withheld. This indemnification obligation is not limited in any way by any limitation on the amount or type of damages or compensation payable to or for Business Associate or its agents under workers' compensation acts, disability benefits acts, or other employee benefit acts.