SUBMITTAL TO THE BOARD OF SUPERV SORS
COUNTY OF RIVERSIDE, STATE OF CALIFORNIA 129

FROM: Riverside County Regional Medical Center (RCRMC), Riverside County Information Technology (RCIT)

SUBMITTAL DATE: January 29, 2015

SUBJECT: Ratify and approve the agreement with MCI Communications Services, Inc. dba Verizon Business Services for a Comprehensive HIPAA Security Risk Analysis and Privacy Assessment Report, other than low bid for the performance period of February 2, 2015 through December 31, 2015, All Districts; [Not to exceed $913,000 total aggregate amount]; (RCRMC Operating Budget)

RECOMMENDED MOTION: That the Board of Supervisors:

1. Ratify and approve the agreement with MCI Communications Services, Inc. dba Verizon Business Services for a Comprehensive HIPAA Security Risk Analysis and Privacy Assessment Report via the competitive bidding process; for the total aggregate amount not to exceed $913,000 February 2, 2015 through December 31, 2015; and
2. Authorize the Purchasing Agent, in accordance with Ordinance No. 459.4, to sign amendments that do not change the substantive terms of the agreement, including amendments to the compensation provision that do not exceed a 10% contingency, for unforeseen project requirements based on the availability of fiscal funds for required services.

RCIT:
Christopher M. Hans, CIO

Zareh Sarrafian
Chief Executive Officer
RCRMC

Sebron K. Partridge
Chief Information Security Officer
RCIT

FINANCIAL DATA	Current Fiscal Year:	Next Fiscal Year:	Total Cost:	Ongoing Cost:	POLICY/CONSENT (per Exec. Office)
COST	$ 830,000	$ 83,000	$ 913,000	$	Consent ☐ Policy ☒
NET COUNTY COST	$ 0	$ 0	$ 0	$ 0	

SOURCE OF FUNDS: RCRMC Operating Budget

Budget Adjustment: No

For Fiscal Year: 14/15 & 15/16

C.E.O. RECOMMENDATION: APPROVE

BY: Debra Cournoyer

County Executive Office Signature

MINUTES OF THE BOARD OF SUPERVISORS

On motion of Supervisor Benoit, seconded by Supervisor Jeffries and duly carried by unanimous vote, IT WAS ORDERED that the above matter is approved as recommended.

Ayes: Jeffries, Tavaglione, Benoit and Ashley
Nays: None
Absent: None
Date: February 10, 2015
xc: RCRMC, Purchasing

Kecia Harper-Ihem
Clerk of the Board
By: Deputy

Prev. Agn. Ref.: | **District:** All | **Agenda Number:** 3-14

PURCHASING & FLEET SERVICES: Lisa Brandl, Director

Departmental Concurrence

FORM APPROVED COUNTY COUNSEL
BY: GREGORY P. PRIAMOS DATE 2/2/15

☐ Positions Added ☐ Change Order
☐ A-30 ☐ 4/5 Vote

BACKGROUND:

Summary

The Department of Health and Human Services requires healthcare organizations such as Riverside County Regional Medical Center and the Community Based Clinics (collectively "County"), to conduct a HIPAA Security Risk Analysis as specified in HIPAA Security Rule 164.308(a)(1). This is a mandatory requirement for healthcare facilities that store or transmit electronic protected health information (ePHI).

The objective of the HIPAA risk analysis is to document any potential risks and vulnerabilities to the privacy, confidentiality, integrity, or availability of protected health information (PHI) at Riverside County Regional Medical Center and the Community Based Clinics. This Analysis includes all electronic media used to create, receive, maintain or transmit ePHI, portable media, desktops and networks. Business Associates and related contracts will also be evaluated to determine the appropriate safeguards to bring the level of risk of exposure of PHI to an acceptable level.

The goal of this project is to obtain a fully-documented HIPAA risk analysis report ("Report") to assist in making informed decisions regarding the appropriate actions needed to secure PHI/ ePHI and achieve County's compliance with applicable federal regulations.

The key final deliverable to be provided is a HIPAA risk analysis report which includes the comprehensive assessment of the controls, processes, and policies used by Riverside County Regional Medical Center and the Community Based Clinics to comply with the HIPAA rules and other laws or regulations.

Impact on Residents and Businesses

The approval of this contract has no negative impact on residents or businesses.

Contract History and Price Reasonableness

On November 26, 2014 Purchasing released Request for Quote (RFQ) #ITARC-314 for a "Comprehensive HIPAA Risk Analysis". A Mandatory bidders meeting was held on December 16, 2014 with sixteen representatives from twelve companies present to discuss the County scope of service and ask questions. At the bid closing on December 23, 2014, the County received eight responses with bid price range from $180,375 to $7,276,680. After thorough review of bid responses and conducting reference checks by the Riverside County Information Security Office to ensure the responses comply with the scope of the requirements, MCI Communications Services, Inc. dba Verizon Business Services was found to be the responsive responsible bidder for the required scope of service for a Comprehensive HIPAA Risk Analysis and Privacy Assessment Report at the cost of $913,000 which includes travel and lodging in the amount not to exceed 10% of the fixed price ($830,000); to be in compliance with County travel policies. Verizon will invoice the actual travel and lodging expenses to the County.

PROFESSIONAL SERVICE AGREEMENT

for

COMPREHENSIVE HIPAA SECURITY RISK ANALYSIS AND PRIVACY ASSESSMENT REPORTS

between

COUNTY OF RIVERSIDE

and

VERIZON BUSINESS NETWORK SERVICES INC., ON BEHALF OF

MCI COMMUNICATIONS SERVICES, INC. DBA VERIZON BUSINESS SERVICES

FEB 10 2015 3-14

TABLE OF CONTENTS

SECTION HEADING

This Agreement, made and entered into this 2nd day of February, 2015, by and between Verizon Business Network Services Inc., on behalf of MCI Communications Services, Inc. dba Verizon Business Services, (herein referred to as "Verizon"), and the COUNTY OF RIVERSIDE, a political subdivision of the State of California, (herein referred to as "COUNTY"). The parties agree as follows:

1. Description of Services

1.1 Verizon shall provide all services as outlined and specified in Exhibit A, Scope of Services, consisting of 5 pages at the prices stated in Exhibit B, Payment Provisions, consisting of 1 page, Exhibit C, Information Security Requirements, consisting of 5 pages, Exhibit D, Confidential Information, consisting of 4 pages (to be delivered to Verizon at initial meeting), Exhibit E, Forms, consisting of 1 page, Exhibit F, preliminary high-level project plan (subject to change as agreed to by the parties), 1 page, and Attachment I, HIPAA Business Associate Attachment to the Agreement, consisting of 12 pages.

1.2 Verizon represents that it has the skills, experience, and knowledge necessary to perform under this Agreement and the COUNTY relies upon this representation. Verizon shall perform to the satisfaction of the COUNTY and in conformance to and consistent with the Scope of Services in Exhibit A and the standards of work for firms/professionals in the same discipline in the State of California.

1.3 Verizon affirms this it is fully apprised of all of the work to be performed under this Agreement; and Verizon agrees it can properly perform this work at the prices stated in Exhibit B. CONTRACTOR is not to perform services or provide products outside of the Agreement.

1.4 Acceptance by the COUNTY of Verizon's performance under this Agreement does not operate as a release of Verizon's responsibility for full compliance with the terms of this Agreement.

2. Period of Performance

2.1 This Agreement shall be effective upon signature of this Agreement by both parties and continues in effect through 12 months after delivery of final reports in accordance with this Agreement, unless terminated earlier. Verizon shall commence performance upon signature of this Agreement by both parties and shall diligently and continuously perform thereafter. The Riverside County Board of Supervisors is the only authority that may obligate the County for a non-cancelable multi-year agreement.

3. Compensation

3.1 The COUNTY shall pay Verizon for services performed, products provided and expenses incurred in accordance with the terms of Exhibit B, Payment Provisions. Maximum payments by COUNTY to Verizon shall not exceed a fixed price total of eight hundred thirty thousand dollars ($830,000) excluding authorized expenses, which will not exceed 10% of the labor total. The fixed price does not include any duties, charges, taxes or expenses which Verizon may be entitled to recover from the COUNTY pursuant to

the Agreement. The parties agree that Verizon's fixed price is based on the requirements stated in this Agreement regardless of the hours of work required. Verizon work beyond the requirements stated shall be subject to additional charges as agreed by the parties in advance in writing.

The COUNTY is not responsible for any fees or costs incurred above or beyond the contracted amount and shall have no obligation to purchase any specified amount of services or products. Unless otherwise specifically stated in Exhibit B, COUNTY shall not be responsible for payment of any of Verizon's expenses related to this Agreement.

3.2 No price increases will be permitted during the first year of this Agreement. All price decreases (for example, if Verizon offers lower prices to another governmental entity) will automatically be extended to the COUNTY. The COUNTY requires written proof satisfactory to COUNTY of cost increases prior to any approved price adjustment. After the first year of the award, a minimum of 30-days advance notice in writing is required to be considered and approved by COUNTY. No retroactive price adjustments will be considered. Any price increases must be stated in a written amendment to this Agreement. The net dollar amount of profit will remain firm during the period of the Agreement. Annual increases shall not exceed the Consumer Price Index- All Consumers, All Items - Greater Los Angeles, Riverside and Orange County areas and be subject to satisfactory performance review by the COUNTY and approved (if needed) for budget funding by the Board of Supervisors.

3.3 Verizon shall be paid only in accordance with an invoice submitted to COUNTY by Verizon, and COUNTY shall pay the invoice within thirty (30) working days from the date of receipt of the invoice. Payment shall be made to Verizon in accordance with the milestones set forth in Exhibit B attached hereto. Prepare invoices in duplicate. For this Agreement, send the original and duplicate copies of invoices to:

Riverside County Information Technology
Attn: Account Payable
3450 14th Street
Riverside, CA 92501

a) Each invoice shall contain a minimum of the following information: invoice number and date; remittance address; bill-to and ship-to addresses of ordering department/division; Agreement number (ITARC-20429-001-12/15); quantities; item descriptions, unit prices, extensions, sales/use tax if applicable, and an invoice total.

b) Invoices shall be rendered monthly in arrears.

3.4 The COUNTY obligation for payment of this Agreement beyond the current fiscal year end is contingent upon and limited by the availability of COUNTY funding from which payment can be made. No legal liability on the part of the COUNTY shall arise for payment beyond June 30 of each calendar year

unless funds are made available for such payment. In the event that such funds are not forthcoming for any reason, COUNTY shall immediately notify Verizon in writing; and this Agreement shall be deemed terminated, have no further force, and effect.

4. Alteration or Changes to the Agreement

4.1 The Board of Supervisors and the COUNTY Purchasing Agent and/or his designee is the only authorized COUNTY representatives who may at any time, by written order, alter this Agreement. If any such alteration causes an increase or decrease in the cost of, or the time required for the performance under this Agreement, an equitable adjustment shall be made in the Agreement price or delivery schedule, or both, and the Agreement shall be modified by written amendment accordingly.

4.2 Any claim by Verizon for additional payment related to this Agreement shall be made in writing by Verizon within 30 days of when Verizon has or should have notice of any actual or claimed change in the work, which results in additional and unanticipated cost to Verizon. If the COUNTY Purchasing Agent decides that the facts provide sufficient justification, he may authorize additional payment to Verizon pursuant to the claim. Nothing in this section shall excuse Verizon from proceeding with performance of the Agreement even if there has been a change.

5. Termination

5.1. COUNTY may terminate this Agreement without cause upon 30 days written notice served upon Verizon stating the extent and effective date of termination.

5.2 COUNTY may, upon five (5) days written notice terminate this Agreement for Verizon's default, if Verizon refuses or fails to comply with the terms of this Agreement or fails to make progress that may endanger performance and does not immediately cure such failure. In the event of such termination, the COUNTY may proceed with the work in any manner deemed proper by COUNTY.

5.3 After receipt of the notice of termination, Verizon shall:

(a) Stop all work under this Agreement on the date specified in the notice of termination; and

(b) Transfer to COUNTY and deliver in the manner as directed by COUNTY any work in process, including materials, reports or other products, which, Verizon shall not be required to complete.

5.4 After termination, COUNTY shall make payment only for Verizon's performance up to the date of termination in accordance with this Agreement.

5.5 Verizon's rights under this Agreement shall terminate (except for fees accrued prior to the date of termination) upon dishonesty or a willful or material breach of this Agreement by Verizon; or in the

event of Verizon's unwillingness or inability for any reason whatsoever to perform the terms of this Agreement. In such event, Verizon shall not be entitled to any further compensation under this Agreement.

5.6 Verizon is not debarred from the System for Award Management (SAM). If the Agreement is federally or State funded, Verizon must notify the COUNTY immediately of a debarment. Reference: System for Award Management (SAM) at https://www.sam.gov for Central Contractor Registry (CCR), Federal Agency Registration (Fedreg), Online Representations and Certifications Application, and Excluded Parties List System (EPLS)). Excluded Parties Listing System (EPLS) (http://www.epls.gov) (Executive Order 12549, 7 CFR Part 3017, 45 CFR Part 76, and 44 CFR Part 17). The System for Award Management (SAM) is the Official U.S. Government system that consolidated the capabilities of CCR/FedReg, ORCA, and EPLS.

5.7 The rights and remedies of COUNTY provided in this section shall not be exclusive and are in addition to any other rights and remedies provided by law or this Agreement.

6. Ownership/Use of Contract Materials and Products

Verizon agrees that, to the extent it is within Verizon's authority, all materials, reports or products in any form, including electronic, first created by Verizon during the term of this Agreement for which Verizon has been compensated by COUNTY pursuant to this Agreement shall be the sole property of the COUNTY. The material, reports or products may be used by the COUNTY for any purpose that the COUNTY deems to be appropriate, including, but not limit to, duplication and/or distribution within the COUNTY or to third parties. Verizon agrees not to release or circulate in whole or part such materials, reports, or products without prior written authorization of the COUNTY. Notwithstanding the foregoing, COUNTY and Verizon acknowledge and agree that Verizon will utilize templates and other intellectual property created by Verizon prior to entering into this Agreement. The parties agree that Verizon (1) will use such templates and other intellectual property as foundational material that is tailored to address Verizon's specific assessment methodology and findings resulting from the work performed hereunder; and (2) retains all rights, title and interest in and to such pre-existing templates and intellectual property (regardless of format), but not to the tailored material and reports containing detailed information about the COUNTY.

7. Conduct of Contractor

7.1 Verizon covenants that it presently has no interest, including, but not limited to, other projects or contracts, and shall not acquire any such interest, direct or indirect, which would conflict in any manner or degree with Verizon's performance under this Agreement. Verizon further covenants that no person or subcontractor having any such interest shall be employed or retained by Verizon under this

Agreement. Verizon agrees to inform the COUNTY of all Verizon's interests, if any, which are or may be perceived as incompatible with the COUNTY's interests.

7.2 Verizon shall not, under circumstances which could be interpreted as an attempt to influence the recipient in the conduct of his/her duties, accept any gratuity or special favor from individuals or firms with whom Verizon is doing business or proposing to do business, in accomplishing the work under this Agreement.

7.3 Verizon or its employees shall not offer gifts, gratuity, favors, and entertainment directly or indirectly to COUNTY employees.

8. Inspection of Service; Quality Control/Assurance

8.1 All performance (which includes services, workmanship, materials, supplies and equipment furnished or utilized in the performance of this Agreement) shall be subject to inspection and test by the COUNTY or other regulatory agencies at all times. Verizon shall provide adequate cooperation to any inspector or other COUNTY representative to permit him/her to determine Verizon's conformity with the terms of this Agreement. If any services performed or products provided by Verizon are not in conformance with the terms of this Agreement, the COUNTY shall have the right to require Verizon to perform the services or provide the products in conformance with the terms of the Agreement at no additional cost to the COUNTY. When the services to be performed or the products to be provided are of such nature that the difference cannot be corrected; the COUNTY shall have the right to: (1) require Verizon immediately to take all necessary steps to ensure future performance in conformity with the terms of the Agreement; and/or (2) reduce the Agreement price to reflect the reduced value of the services performed or products provided. The COUNTY may also terminate this Agreement for default and charge to Verizon any costs incurred by the COUNTY because of Verizon's failure to perform.

8.2 Verizon shall establish adequate procedures for self-monitoring and quality control and assurance to ensure proper performance under this Agreement; and shall permit a COUNTY representative or other regulatory official to monitor, assess, or evaluate Verizon's performance under this Agreement at any time, upon reasonable notice to the Verizon.

9. Independent Contractor/Employment Eligibility

9.1 Verizon is, for purposes relating to this Agreement, an independent contractor and shall not be deemed an employee of the COUNTY. It is expressly understood and agreed that Verizon (including its employees, agents, and subcontractors) shall in no event be entitled to any benefits to which COUNTY employees are entitled, including but not limited to overtime, any retirement benefits, worker's compensation benefits, and injury leave or other leave benefits. There shall be no employer-employee

relationship between the parties; and Verizon shall hold COUNTY harmless from any and all claims that may be made against COUNTY based upon any contention by a third party that an employer-employee relationship exists by reason of this Agreement. It is further understood and agreed by the parties that Verizon in the performance of this Agreement is subject to the control or direction of COUNTY merely as to the results to be accomplished and not as to the means and methods for accomplishing the results.

9.2 Verizon warrants that it shall make all reasonable efforts to fully comply with all federal and state statutes and regulations regarding the employment of aliens and others and to ensure that employees performing work under this Agreement meet the citizenship or alien status requirement set forth in federal statutes and regulations. Verizon shall obtain, from all employees performing work hereunder, all verification and other documentation of employment eligibility status required by federal or state statutes and regulations including, but not limited to, the Immigration Reform and Control Act of 1986, 8 U.S.C. §1324 et seq., as they currently exist and as they may be hereafter amended. Verizon shall retain all such documentation for all covered employees, for the period prescribed by the law.

9.3 Ineligible Person shall be any individual or entity who: Is currently excluded, suspended, debarred or otherwise ineligible to participate in the federal health care programs; or has been convicted of a criminal offense related to the provision of health care items or services and has not been reinstated in the federal health care programs after a period of exclusion, suspension, debarment, or ineligibility.

9.4 Verizon shall use Live Scan to screen prospective Covered Individuals prior to hire or engagement. Verizon shall not hire or engage any Ineligible Person to provide services directly relative to this Agreement. Verizon shall screen all current Covered Individuals immediately after execution of this Agreement to ensure that they have not become Ineligible Persons unless Verizon has performed such screening on same Covered Individuals under a separate agreement with COUNTY within the past six (6) months. Covered Individuals shall be required to disclose to Verizon immediately any debarment, exclusion or other event that makes the Covered Individual an Ineligible Person. Verizon shall notify COUNTY within five (5) business days after it becomes aware if a Covered Individual providing services directly relative to this Agreement becomes debarred, excluded or otherwise becomes an Ineligible Person.

9.5 Verizon acknowledges that Ineligible Persons are precluded from providing federal and state funded health care services by contract with COUNTY in the event that they are currently sanctioned or excluded by a federal or state law enforcement regulatory or licensing agency. If Verizon becomes aware that a Covered Individual has become an Ineligible Person, Verizon shall remove such individual from responsibility for, or involvement with, COUNTY business operations related to this Agreement.

9.6 Verizon shall notify COUNTY within five (5) business days if a Covered Individual or entity is currently excluded, suspended or debarred, or is identified as such after being sanction screened. Such individual or entity shall be promptly removed from participating in any activity associated with this Agreement.

10. Subcontract for Work or Services

No contract shall be made by Verizon with any other party for furnishing any of the work or services under this Agreement without the prior written approval of the COUNTY; but this provision shall not require the approval of contracts of employment between Verizon and personnel assigned under this Agreement, or for parties named in the proposal and agreed to under this Agreement. County shall not unreasonably withhold its approval of Verizon's subcontractors.

11. Disputes

11.1 The parties shall attempt to resolve any disputes amicably at the working level. If that is not successful, the dispute shall be referred to the senior management of the parties. Any dispute relating to this Agreement, which is not resolved by the parties, shall be decided by the COUNTY's Purchasing Department's Compliance Contract Officer who shall furnish the decision in writing. The decision of the COUNTY's Compliance Contract Officer shall be final and conclusive unless determined by a court of competent jurisdiction to have been fraudulent, capricious, arbitrary, or so grossly erroneous to imply bad faith. Verizon shall proceed diligently with the performance of this Agreement pending the resolution of a dispute.

11.2 Prior to the filing of any legal action related to this Agreement, the parties shall be obligated to attend a mediation session in Riverside County before a neutral third party mediator. A second mediation session shall be required if the first session is not successful. The parties shall share the cost of the mediations.

12. Licensing and Permits

Verizon shall comply with all State or other licensing requirements, including but not limited to the provisions of Chapter 9 of Division 3 of the Business and Professions Code. All licensing requirements shall be met at the time proposals are submitted to the COUNTY. Verizon warrants that it has all necessary permits, approvals, certificates, waivers and exemptions necessary for performance of this Agreement as required by the laws and regulations of the United States, the State of California, the County of Riverside and all other governmental agencies with jurisdiction, and shall maintain these throughout the term of this Agreement.

13. Use By Other Political Entities

Verizon agrees to extend the same pricing, terms, and conditions as stated in this Agreement to each and every political entity, special district, and related non-profit entity in Riverside County. It is understood that other entities shall make purchases in their own name, make direct payment, and be liable directly to Verizon; and COUNTY shall in no way be responsible to Verizon for other entities' purchases.

14. Non-Discrimination

Verizon shall not be discriminate in the provision of services, allocation of benefits, accommodation in facilities, or employment of personnel on the basis of ethnic group identification, race, religious creed, color, national origin, ancestry, physical handicap, medical condition, marital status or sex in the performance of this Agreement; and, to the extent they shall be found to be applicable hereto, shall comply with the provisions of the California Fair Employment and Housing Act (Gov. Code 12900 et. seq), the Federal Civil Rights Act of 1964 (P.L. 88-352), the Americans with Disabilities Act of 1990 (42 U.S.C. S1210 et seq.) and all other applicable laws or regulations.

15. Records and Documents

Verizon shall make available, upon written request by any duly authorized Federal, State, or COUNTY agency, a copy of this Agreement and such books, documents and records as are necessary to certify the nature and extent of Verizon's costs related to this Agreement. All such books, documents and records shall be maintained by Verizon for at least five years following termination of this Agreement and be available for audit by the COUNTY. Verizon shall provide to the COUNTY reports and information related to this Agreement as requested by COUNTY.

16. Confidentiality

16.1 Verizon shall not use for personal gain or make other improper use of privileged or confidential information which is acquired in connection with this Agreement. Confidential information stored on or transmitted to/from digital systems shall be encrypted at minimum to meet Federal Information Processing Standard (FIPS) Publication 140-2 while at rest and in transit. The term "digital systems" includes but is not limited to: computing systems, servers, personal computers, laptops, cell phones/smartphones, tablets, thumb or flash drives, external hard drives and all other devices that can store or transmit digital data. The term "privileged or confidential information" includes but is not limited to: unpublished or sensitive technological or scientific information; medical, personnel, or security records; anticipated material requirements or pricing/purchasing actions; COUNTY information or data which is not subject to public disclosure; COUNTY operational procedures; electronic data; and knowledge of selection of contractors, subcontractors or suppliers in advance of official announcement.

16.2 Verizon shall protect from unauthorized disclosure names and other identifying information concerning persons receiving services pursuant to this Agreement, except for general statistical information not identifying any person. Verizon shall not use such information for any purpose other than carrying out Verizon's obligations under this Agreement. Verizon shall promptly transmit to the COUNTY all third party requests for disclosure of such information. Verizon shall not disclose, except as otherwise specifically permitted by this Agreement or authorized in advance in writing by the COUNTY, any such information to anyone other than the COUNTY. For purposes of this paragraph, identity shall include, but not be limited to, name, identifying number, symbol, or other identifying particulars assigned to the individual, such as finger or voice print or a photograph.

16.3 Verizon is subject to and shall operate in compliance with all relevant requirements contained in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, enacted August 21, 1996, and the related laws and regulations promulgated subsequent thereto. Please refer to Attachment 1 of this Agreement.

16.4 All information, data and documents received by Verizon from the COUNTY (regardless of format) pursuant to this Agreement shall be maintained in strict confidence by Verizon and not be disclosed to any third party.

16.5 Notwithstanding the confidentiality obligations required herein, Verizon's confidentiality obligations hereunder shall not apply to information which: (a) is already known to Verizon (other than the terms of this Agreement); (b) becomes publicly available without fault of Verizon; (c) is rightfully obtained by Verizon from a third party without restriction as to disclosure, or such confidential information is approved for release by written authorization of the COUNTY; (d) is developed independently by Verizon without use of the COUNTY's confidential information; or (e) is required to be disclosed by law, provided that prior to making such required disclosure, Verizon shall notify the COUNTY that disclosure is legally required.

16.6 All information, data and documents prepared by Verizon (regardless of format) is being prepared pursuant to and shall be subject to California Evidence Code 1157.

17. Administration/Contract Liaison

The COUNTY Chief Information Security Officer (CISO), or designee, shall administer this Agreement on behalf of the COUNTY. The CISO is to serve as the liaison with Verizon in connection with this Agreement.

18. Notices

All correspondence and notices required or contemplated by this Agreement shall be delivered to the respective parties at the addresses set forth below and are deemed submitted two days after their deposit in the United States mail, postage prepaid:

COUNTY OF RIVERSIDE

Purchasing and Fleet Services
Attn: Rick Hai
2980 Washington Street
Riverside, CA 92504

VERIZON

Verizon Business Services
Attn: Stephen Pruneri
18850 Orange Street
Bloomington, CA 92316

Riverside County Information Security Office
Attn: CISO
Suite 5
3450 14th Street
Riverside, CA 92501

Office of the County Counsel
Asst. County Counsel Anita Willis
3960 Orange St.
Suite 500
Riverside, CA 92501

19. Force Majeure

If either party is unable to comply with any provision of this Agreement due to causes beyond its reasonable control, and which could not have been reasonably anticipated, such as acts of God, acts of war, civil disorders, or other similar acts, such party shall not be held liable for such failure to comply.

20. EDD Reporting Requirements

In order to comply with child support enforcement requirements of the State of California, the COUNTY may be required to submit a Report of Independent Contractor(s) form **DE 542** to the Employment Development Department. Verizon agrees to furnish the required data and certifications to the COUNTY within 10 days of notification of award of Agreement when required by the EDD. This data will be transmitted to governmental agencies charged with the establishment and enforcement of child support orders. Failure of Verizon to timely submit the data and/or certificates required may result in the contract

being awarded to another contractor. In the event a contract has been issued, failure of Verizon to comply with all federal and state reporting requirements for child support enforcement or to comply with all lawfully served Wage and Earnings Assignments Orders and Notices of Assignment shall constitute a material breach of Agreement. If Verizon has any questions concerning this reporting requirement, please call (916) 657-0529. Verizon should also contact its local Employment Tax Customer Service Office listed in the telephone directory in the State Government section under "Employment Development Department" or access their Internet site at www.edd.ca.gov.

21. Hold Harmless/Indemnification

21.1 Verizon shall indemnify and hold harmless the County of Riverside, its Agencies, Districts, Special Districts and Departments, their respective directors, officers, Board of Supervisors, elected and appointed officials, employees, agents and representatives (individually and collectively hereinafter referred to as Indemnitees) from any liability, action, claim or damage whatsoever, based or asserted upon the negligence or willful misconduct of Verizon, its officers, employees, subcontractors, agents or representatives arising out of or in any way relating to this Agreement, including but not limited to property damage, bodily injury, or death or any other element of any kind or nature. Verizon shall defend, at its sole expense up to a maximum aggregate liability for all claims hereunder equal to the total fees paid or payable by the County of Riverside to Verizon under this Agreement, all costs, and fees including, but not limited, to attorney fees, cost of investigation, defense and settlements or awards, the Indemnitees in any claim or action based upon such alleged acts or omissions.

21.2 With respect to any action or claim subject to indemnification herein by Verizon, Verizon shall, at their sole cost, have the right to use counsel of their own choice and shall have the right to adjust, settle, or compromise any such action or claim without the prior consent of COUNTY; provided, however, that any such adjustment, settlement or compromise in no manner whatsoever limits or circumscribes Verizon's indemnification to Indemnitees as set forth herein.

21.3 Verizon's obligation hereunder shall be satisfied when Verizon has provided to COUNTY the appropriate form of dismissal relieving COUNTY from any liability for the action or claim involved.

21.4 The specified insurance limits required in this Agreement shall in no way limit or circumscribe Verizon's obligations to indemnify and hold harmless the Indemnitees herein from third party claims.

22. Insurance

22.1 Without limiting or diminishing Verizon's obligation to indemnify or hold the COUNTY harmless, Verizon shall procure and maintain or cause to be maintained, at its sole cost and expense, the

following insurance coverage's during the term of this Agreement. As respects to the insurance section only, the COUNTY herein refers to the County of Riverside, its Agencies, Districts, Special Districts, and Departments, their respective directors, officers, Board of Supervisors, employees, elected or appointed officials, agents, or representatives as Additional Insureds.

A. Workers' Compensation:

If Verizon has employees as defined by the State of California, Verizon shall maintain statutory Workers' Compensation Insurance (Coverage A) as prescribed by the laws of the State of California. Policy shall include Employers' Liability (Coverage B) including Occupational Disease with limits not less than $1,000,000 per person per accident. The policy shall waive subrogation in favor of The County of Riverside.

B. Commercial General Liability:

Commercial General Liability insurance coverage, including but not limited to, premises-operations contractual liability, products and completed operations liability, personal and advertising injury, and cross liability coverage, covering claims which may arise from or out of Verizon's performance of its obligations hereunder. Policy shall include the COUNTY as Additional Insured as their interest may appear. Policy's limit of liability shall not be less than $1,000,000 per occurrence combined single limit. If such insurance contains a general aggregate limit, it shall apply separately to this agreement or be no less than two (2) times the occurrence limit.

C. Vehicle Liability:

If vehicles are used in the performance of the obligations under this Agreement, then Verizon shall maintain commercial automobile liability insurance for all owned, non-owned, or hired vehicles so used in an amount not less than $1,000,000 per occurrence combined single limit each accident for bodily injury and property damage. Policy shall include the COUNTY as Additional Insureds as their interest may appear.

D. Professional Liability

Verizon shall maintain Professional Liability Insurance providing coverage for Verizon's performance of professional work included within this Agreement, with a limit of liability of not less than $1,000,000 per occurrence and $2,000,000 per claim and aggregate. If Verizon's Professional Liability Insurance is written on a claims made basis rather than an occurrence basis, such insurance shall continue through the term of this Agreement and Verizon shall purchase at his sole expense either 1) an Extended Reporting Endorsement (also, known as Tail Coverage); or 2) Prior Dates Coverage from new insurer with a retroactive date back to the date of, or prior to, the inception of this Agreement; or 3) demonstrate through Certificates of Insurance that Verizon has Maintained continuous coverage with the same or original insurer.

E. General Insurance Provisions - All lines:

1) Any insurance carrier providing insurance coverage hereunder shall be admitted to the State of California and have an A M BEST rating of not less than A: VIII (A:8) unless such requirements are waived, in writing, by the County Risk Manager. If the County's Risk Manager waives a requirement for a particular insurer such waiver is only valid for that specific insurer and only for one policy term.

2) Verizon shall cause Verizon's insurance carrier(s) to furnish the County of Riverside with a properly executed original Certificate(s) of Insurance evidencing coverage as required herein. In the event of cancellation or expiration, this Agreement shall terminate forthwith, unless the County of Riverside receives, within thirty (30) days of such renewal or expiration, another properly executed original Certificate of Insurance. Verizon shall not commence operations until COUNTY has been furnished original Certificate (s) of Insurance. An individual authorized by the insurance carrier shall sign the Certificate of Insurance.

3) It is understood and agreed to by the parties hereto that Verizon's insurance shall be construed as primary insurance, and the COUNTY'S insurance and/or deductibles and/or self-insured retention's or self-insured programs shall not be construed as contributory.

4) If, during the term of this Agreement or any extension thereof, there is a material change in the scope of services; or, there is a material change in the equipment to be used in the performance of the scope of work; or, the term of this Agreement, including any extensions thereof, exceeds five (5) years; the COUNTY reserves the right to adjust the types of insurance and the limits of liability required under this Agreement, if in the County Risk Manager's reasonable judgment, the amount or type of insurance carried by Verizon has become inadequate.

5) Verizon shall pass down the insurance obligations contained herein to all tiers of subcontractors working under this Agreement.

7) The insurance requirements contained in this Agreement may be met with a program(s) of self-insurance reasonably acceptable to COUNTY.

8) Verizon agrees to notify COUNTY of any claim by a third party or any incident or event that may give rise to a claim arising from the performance of this Agreement.

23. General

23.1 Verizon shall not delegate or assign any interest in this Agreement, whether by operation of law or otherwise, without the prior written consent of COUNTY. Any attempt to delegate or assign any interest herein shall be deemed void and of no force or effect.

23.2 Any waiver by COUNTY of any breach of any one or more of the terms of this Agreement shall not be construed to be a waiver of any subsequent or other breach of the same or of any other term of this Agreement. Failure on the part of COUNTY to require exact, full, and complete compliance with any

terms of this Agreement shall not be construed as in any manner changing the terms or preventing COUNTY from enforcement of the terms of this Agreement.

23.3 In the event Verizon receives payment under this Agreement, which is later disallowed by COUNTY for material nonconformance with the terms of the Agreement, the Verizon shall promptly refund or issue a credit to COUNTY for the disallowed amount to COUNTY on request of COUNTY.

23.4 Verizon shall not provide partial delivery or shipment of services or products unless specifically stated in the Agreement.

23.5 Verizon shall not provide any services or products subject to any chattel mortgage or under a conditional sales contract or other agreement by which an interest is retained by a third party. Verizon warrants that it has good title to all materials or products used by Verizon or provided to COUNTY pursuant to this Agreement, free from all liens, claims, or encumbrances.

23.6 Nothing in this Agreement shall prohibit the COUNTY from acquiring the same type or equivalent equipment, products, materials or services from other sources, when deemed by the COUNTY to be in its best interest. The COUNTY reserves the right to purchase more or less than the quantities specified in this Agreement.

23.7 The COUNTY agrees to cooperate with Verizon in Verizon's performance under this Agreement, including, if stated in the Agreement, providing Verizon with reasonable facilities and timely access to COUNTY data, information, and personnel.

23.8 Verizon shall comply with all applicable Federal, State and local laws and regulations. Verizon shall comply with all applicable COUNTY policies and procedures. In the event that there is a conflict between the various laws or regulations that may apply, Verizon shall comply with the more restrictive law or regulation.

23.9 Verizon shall comply with all air pollution control, water pollution, safety and health ordinances, statutes, or regulations, which apply to performance under this Agreement.

23.10 Verizon shall comply with all requirements of the Occupational Safety and Health Administration (OSHA) standards and codes as set forth by the U.S. Department of Labor and the State of California (Cal/OSHA).

23.11 This Agreement shall be governed by the laws of the State of California. Any legal action related to the performance or interpretation of this Agreement shall be filed only in the Superior Court of the State of California located in Riverside, California, and the parties waive any provision of law providing for a change of venue to another location. In the event any provision in this Agreement is held by a court of competent jurisdiction to be invalid, void, or unenforceable, the remaining provisions will nevertheless continue in full force without being impaired or invalidated in any way.

23.12 This Agreement, including any attachments or exhibits, constitutes the entire Agreement of the parties with respect to its subject matter and supersedes all prior and contemporaneous representations, proposals, discussions and communications, whether oral or in writing. This Agreement may be changed or modified only by a written amendment signed by authorized representatives of both parties.

COUNTY:

Signature: Marion Ashley

Print Name: Marion Ashley

Title: Chairman, Board of Supervisors

Dated: FEB 10 2015

FORM APPROVED COUNTY COUNSEL
BY: ANITA C. WILLIS 2-2-15 DATE

ATTEST:
KECIA HARPER-IHEM, Clerk
By: DEPUTY

VERIZON BUSINESS NETWORK SERVICES INC., ON BEHALF OF MCI COMMUNICATIONS SERVICES, INC. DBA VERIZON BUSINESS SERVICES:

Signature: Anthony Recine

Print Name: Anthony Recine

Title: Senior Vice President and Chief Marketing Officer

Dated: 1/30/2015

Exhibit A
Scope of Service

1. General Requirements

1.1 The Department of Health and Human Services requires healthcare organizations such as Riverside County Regional Medical Center, and the Community Based Clinics (collectively "County"), which includes the locations listed in Section 2.1.5, to conduct a **HIPAA risk analysis** as specified in HIPAA Security Rule 164.308(a)(1). This is a mandatory requirement for healthcare facilities that store or transmit electronic protected health information (ePHI).

The objective of the HIPAA risk analysis to be done by Verizon pursuant to this Agreement ("Analysis") is to document any potential risks and vulnerabilities to the privacy, confidentiality, integrity, or availability of protected health information (PHI) at Riverside County Regional Medical Center and the Community Based Clinics. This Analysis includes all electronic media used to create, receive, maintain or transmit ePHI, portable media, desktops and networks. Business Associates shall be evaluated to determine the safeguards that are in place or not in place relative to the OCR Audit Protocol and the County Business Associate template. .

The goal of this Agreement with Verizon is for the County to receive a comprehensive, fully-documented HIPAA risk analysis report ("Report") to assist in making informed decisions regarding the appropriate actions needed to secure PHI/ ePHI and achieve County's compliance with applicable federal regulations.

The key final deliverable to be provided by Verizon is a HIPAA risk analysis report which includes the comprehensive assessment of the controls, processes, and policies used by Riverside County Regional Medical Center and the Community Based Clinics to comply with the HIPAA rules and other laws or regulations. The risk analysis methodology used by Verizon shall align to the NIST 800-30 framework and the OCR audit protocol, which contains the requirements and assessment procedures based on the following performance criteria:

A. All requirements for the Breach Notification Rule;

B. All Security Rule requirements for:

Administrative Safeguards

- Risk analysis procedures and demonstration of a risk management process;
- Policies and procedures relevant to operational security, including business associate security requirements;
- Information access restriction requirements and controls;
- Incident response procedures and disaster recovery plan and;
- Evidence of periodic technical and non-technical reviews.

Physical Safeguards

- Physical access controls, such as building access and appropriate record keeping;
- Policies and procedures for workstation security; and
- Proper usage, storage, and disposal of data storage devices

Technical Safeguards

- Auditing and audit procedures;
- Use of encryption devices and tools; and
- Implementation of technology to ensure ePHI confidentiality, integrity, and availability

C. Privacy Rule requirements for:

- Notice of Privacy Practices for PHI;
- Rights to request privacy protections for PHI;
- Individual access to PHI;
- Administrative requirements;
- Uses and disclosures of PHI;
- Amendment of PHI; and
- Accounting of disclosures

Verizon's activities in conducting the HIPAA risk analysis shall include but not necessarily be limited to the following:

A. Data collection to locate where PHI/ePHI is being stored, received, maintained or transmitted. This may include, but not be limited to, written surveys and interviews of management and staff, direct observation of processes, reviews of policies, procedures, logs, and other relevant documentation, and walk through inspections of physical environment.
B. Assessment of current security measures in place to protect PHI/ePHI.
C. Assessment of County IT assets that store, receive, maintain or transmit ePHI, facilities, policies and procedures, and the privacy and security controls alignment with the County's HIPAA and HITECH requirements.
D. Identification and documentation of potential threats and vulnerabilities to each information asset class.
E. Determination of the likelihood of threat occurrence and of the potential impact (for example, how many people could be affected, or to what extent private data could be exposed).
F. Determination of the level of risk and recommendations to mitigate risk.
G. Finalized documentation and a formal report of the results.
H. Formal on-site presentation to County senior management of findings and recommendations.

All draft and final reports prepared pursuant to this Agreement (regardless of format) shall be: (1) provided to County CISO at the addresses set forth in the Agreement; and (2) be subject to the attorney work product privilege pursuant to applicable law.

1.2 Primary Location of Service

Verizon shall provide services during normal business hours (Monday through Friday, 8:00 AM to 4:30 PM Pacific Time) at:

Riverside County Regional Medical Center (RCRMC),
26520 Cactus Ave, Moreno Valley, CA 92555

1.3 HIPAA Risk Analysis

The Analysis shall be performed as required by this SOW and be based on the standards listed herein.

Verizon shall:

- Conduct the Analysis in accordance with the requirements set forth by 45 CFR 164.308(a)(1), NIST 800-30, NIST 800-66, NIST 800-53, the HIPAA regulations pursuant to 45 CFR Part 160 and Subparts A and E of Part 164.
- Assess each of the 165 HIPAA audit protocols as identified by the Office of Civil Rights (OCR) Audit Protocol – specifically addressing each of the 5 components (Administrative, Physical, Technical, Policies and Procedures, Operational Standards).
- Evaluate the current physical and electronic PHI handling and monitoring practices against the requirements of HIPAA regulations and identify gaps between current practices and required practices under HIPAA regulations.
- Assess all Analysis activities aligned to the current NIST SP 800-30 framework (see exhibit E).
- Develop a Corrective Action Plan (CAP) which documents in plain language each gap, and Verizon's recommendations for remediation. The final Report shall identify findings and remediation specific to County, and be customized and tailored to support County's alignment with HIPAA and HITECH requirements.

2 Scope Requirements

2.1 In-Scope

Type	Quantity
2.1.1 Computing systems include but are not limited to: Desktops and Laptops; Tablets; Servers; Storage/Backup; Email System; Audio Visual; Printers and Copiers; Fax Machines; Multifunctional Printers; Video Teleconferencing; Cell Phones	5,000
2.1.2 Network Devices include but are not limited to: Routers, Switches and Firewalls; VPNs, RSA Tokens, and Remote Access Configurations; PBX and VOIP, and Wireless	250
2.1.3 Data Centers/ePHI Repositories	12
2.1.4 Information Exchanges/Programs/Affiliates	60
2.1.5 Locations include but are not limited to: 1. Banning Family Care Center - 3055 W. Ramsey, Banning, CA 92220 2. Blythe Family Health Clinic - 321 W. Hobson way, Blythe, CA 92225 3. Corona Family Care Center - 505 S. Buena Vista Ave. Suite #101, Corona, CA 92882 4. Hemet Family Care Center - 880 N. State St., Hemet CA 92543 5. Indio Family Care Center - 47-923 Oasis St., Indio, CA 92201 6. Jurupa Family Care Center - 9415 Mission Blvd., Riverside, CA 92509 7. Lake Elsinore Family Care Center - 2499 E. Lakeshore Drive, Lake Elsinore, CA 92530 8. Mecca Family Health Clinic - 91275 66th Avenue Suite 500, Mecca, CA 92254 9. Palm Springs Family Care Center - 1515 North Sunrise Way, Palm Springs, CA 92262 10. Perris Family Care Center - 308 E. San Jacinto Ave., Perris CA 92570 11. Riverside Neighborhood Health Center - 7140 Indiana Ave., Riverside, CA 92504 12. Rubidoux Family Care Center - 5256 Mission Blvd., Riverside, CA 92509 13. RCRMC Hospital, Moreno Valley, CA 14. RCRMC CPC, Moreno Valley, CA 15. Arlington Campus, Riverside, CA	30

16. Education Building, RCRMC Campus, Moreno Valley, CA 17. Pharmacy within RCRMC Hospital, Moreno Valley, CA 18. Renaissance Radiology 19. Robert Presley Detention Facility, 4000 Orange St. Riverside California. 92501 20. Southwest Juvenile Hall 30755 Auld Rd., Murrieta California 92563 21. Smith Correctional Facility 627 Hargrave St., Banning California. 92220 22. Indio Jail, 46057 Oasis St., Indio California 92201 23. Blythe Jail, 216 North Spring St., Blythe California 92225 24. Mobile Health Unit Riverside Juvenile Hall, 3933 Harrison St., Riverside California 92503 25. Indio Juvenile Hall, 47665 Oasis St., Indio California 92201 26. Southwest Justice Center, 30755 Auld Rd., Murrieta California 92563 27. Riverside County Innovation Center – Data Center 3450 H Street, Riverside, CA 92501 28. RC3 Data Center, 1960 Chicago, Bldg. F, Riverside, CA 92501 3450	
2.1.6 Software Applications	300
2.1.7 Vendor Contracts	450

2.2 Cost to Exceed

Any number of identified units that exceed the quantity defined above shall be presented to the CISO for review and inclusion in this effort via the Verizon change order process.

2.3 Out of Scope

The following items are outside the scope of services that Verizon is required to perform under this Agreement:

a) Inputs to and outputs from, the above, which are outside of the County control.
b) Other products, services, or applications not listed in this Agreement.
c) International IT or other offshore administrative support, not listed in this Agreement.
d) Any form of physical or logical changes to County's environment; from the date that element was assessed.
e) Any other scope not specifically and expressly described in this Agreement.
f) Technical or Operational Testing of security or privacy controls.

Verizon is willing to provide additional support, information and details to the County and to any third party (as authorized in writing by the County) on a Time-and-Material basis to describe the scope of and manner in which Verizon conducted the Comprehensive HIPAA Risk Analysis and Security Assessment under this Agreement and any additional regulatory review and compliance guidance requested by the County.

3. Project Approach

3.1. Program Management

Verizon shall assign a Project Manager (PM) who will work with the County's project manager. Verizon's PM shall provide a secure portal for confidential document transfers. Verizon shall produce and provide a project plan using Microsoft Project which shall identify tasks and related resources. Verizon shall conduct a Project kickoff with the County team and business and IT stakeholders. Verizon's PM shall conduct daily status updates via updated project plan and shall provide access to plan in addition to a weekly executive report. The Verizon PM shall work with the County's PM daily to resolve issues and keep the work on schedule and notify the County promptly of schedule changes. Refer to Exhibit F for preliminary project plan.

3.2. Document Review

Using the secure portal provided above, Verizon shall request and review all the County provided documentation and data related to the scope defined in this Agreement. Verizon shall also gather reasonable amounts of information related to, but not limited to, policies, processes, and procedures, logs, forms, vulnerability scanning report and working documents as part of the analysis and assessment being performed under this Agreement. Verizon shall review the County's Policies and Procedures for their alignment to the HIPAA Requirements and sufficiency to protect PHI and ePHI. Where Policy or Procedure gaps are identified, Verizon shall identify the Policies and Procedures necessary to achieve best alignment and to support data protection and confidentiality.

3.3. Interviews and Onsite Inspections

Verizon shall request and conduct onsite interviews with all required County management, staff members, and other key stakeholders regarding HIPAA requirements. The County shall assist in setting up and coordinating interviews. Verizon shall conduct onsite inspections (formal and informal walk-thru's) of in-scope locations. Verizon shall leverage interviews and onsite observations to evaluate physical security controls.

3.4. Assessment

Verizon shall conduct a HIPAA Security Risk and Privacy Assessment in accordance with the County's requirements as defined in this Agreement. Verizon shall assess and document the alignment of the County's security and privacy controls requirements. Verizon shall form conclusions as to the County's alignment with their security and privacy requirements, and provide recommendations to improve that alignment. Verizon shall conduct its assessment using the 165 HIPAA audit protocols as identified by the Office of Civil Rights (OCR) Audit Protocol. Verizon shall:

- Assess implementation of security controls including documentation review, interview of key stakeholders and staff, operational observation of control processes.
- Review the performance of security controls at the facilities, to support validating implementation of the security controls.
- Review available logs in order to determine the effectiveness of security controls in County systems. Evaluate the current physical and ePHI-handling and monitoring practices against the County's requirements.
- Do a gap analysis of and assess the Business Associate Agreements with the County's vendors that are contracted to access, store, or transmit ePHI.

- Review initial findings with County to identify potential errors or omissions in initial finding results.
- Review all software applications that access, store or transmit ePHI against the requirements of the OCR Audit Protocol. Identify gaps between current practices and required/addressable controls.
- Provide findings, conclusions, and recommendations as to the County's overall and facility alignment with the County's security requirements.
- Evaluate any residual risks. Evaluate options for changes to County's current practices in order to align the County with OCR audit protocols.

3.5 Assessment Reporting

Verizon shall document the testing procedures, testing results, findings, conclusions, and recommendations in a DRAFT Report relevant to the specific circumstances of the County. Based on agreed-to comments, Verizon shall prepare and deliver the FINAL Report for the County via Verizon's secure portal. Verizon understands that the desired target date for draft Reports is April 22, 2015, which includes all the evidence collected during the assessment process, with final Reports provided on or before May 1, 2015. Verizon shall use commercially reasonable efforts to meet those dates in light of the scope and complexity of the assessment.

Verizon shall provide a high level executive summary presentation of the overall assessment findings and recommendations upon completion of the final report. The date of the presentation will be specified at a mutually agreed upon time between Verizon and the County.

3.6 Deliverables and Documentation to be produced by Verizon.

3.6.1 Verizon shall document our testing results, findings, conclusions, and recommendations in an SRA report. The report shall provide an executive summary, and introduction to the project and major results, outline the County's requirements and Verizon's findings relative the County's alignment to the County's security and privacy requirements. Verizon shall provide tactical and strategic recommendations to better align the County's security and privacy controls with the County's requirements.

3.6.2 Verizon shall develop and provide a Corrective Action Plan (CAP) that provides recommendations designed to best align the County with the OCR audit protocols, and to void, reduce, or control the residual risks identified during the risk assessment. The CAP shall include, but not be limited to recommending improvements in security and compliance governance and policy, projects to improve secure operating processes, and projects to improve technical controls. For the avoidance of doubt, Verizon is relying on any and all County information, which is provided to it by the County in its creation of the deliverables and documentation described herein. Verizon shall not go outside of the County to independently validate any of the information provided to it by the County and shall be entitled to rely on such information.

3.6.3 Verizon shall provide deliverables in PDF, and in MS Word. Delivered Data shall be provided in MS Excel (XLS, and/or CSV formats). A list of deliverables is as follows:

A. MS Project Plan at the Kickoff
B. Findings Review presentation to management(Security and Privacy)
C. Draft Final Reports (to include all elements of Final Reports, Security and Privacy)
D. Final Reports:
    1. HIPAA Privacy and Breach Assessment Final Report

a) Executive Summary
b) Introduction and Project scope
c) Project Approach and procedures applied during assessment
d) Conclusions relevant to the circumstances of the organization, covering potential risk measurements.
e) Organize findings by facility.
f) Conclusions as to Healthcare privacy policy and procedures gaps, and recommendations for gap-filling policies and procedures (Refer to Section 3.2)
g) A listing of vulnerabilities, provided by County vulnerability assessment reports, and threats as deemed appropriate by Verizon.
h) Privacy and Breach Assessment findings
i) Finding for each OCR Audit Protocol shall be documented as to their "In-Place/"Not-In-Place" state.
j) Recommendations for risk mitigation and for improvement of the County's alignment to OCR audit protocols.
k) A Corrective Action Plan (CAP)
l) MS Project Plan completed, and inventory of all materials used.

2. HIPAA Security Risk Analysis Final Report
   a) Executive Summary
   b) Introduction and Project scope
   c) Project Approach and procedures applied during assessment
   d) Conclusions as to the County's alignment with the OCR Audit Protocol.
   e) Organize findings by facility.
   f) Conclusions as to Healthcare Security and Privacy Policy and Procedures gaps, and recommendations for gap-filling policies and procedures (Refer to Section 3.2)
   g) An inventory of IT resources potentially exposed to ePHI, hosted services maintaining ePHI, and PHI movement within the organization as can be determined from information provided by application and IT resource owners.
   h) Review software applications that access, store or transmit ePHI against requirements of the OCR Audit protocol.
   i) An inventory of the County's Vendors relative to their PHI-exposure and BAA status to understand PHI movement between the County and Vendors.
   j) An inventory of business partners relative to PHI-exposure and protection agreements status to understand PHI movement between the County and business partners
   k) A listing of vulnerabilities, provided by County vulnerability assessment reports, and threats as deemed appropriate by Verizon.
   l) Provide semi-qualitative risk rating in accordance with NIST SP 800-30 for each performance criteria as defined in OCR Audit Protocol
   m) Security Assessment Findings
   n) Finding for each OCR Audit Protocol shall be documented as to their "In-Place/"Not-In-Place"
      i. Include OCR Audit Protocol and testing methodology
      ii. Actual results/findings to include the name of the location to which they apply.

o) Recommendations for risk mitigation and for improvement of the County's alignment to OCR audit protocols.
p) Develop a Corrective Action Plan (CAP) based on OCR Audit Protocol findings identified during the HIPAA SRA. Identified control deficiencies in the CAP shall be associated to a remediation recommendation that addresses an OCR Audit Protocol requirement. Remediation recommendations shall describe estimated cost, resources and timelines associated with each recommendation.
q) Where applicable provide existing samples of policies, procedures, guidelines, references, run books and handbooks to help mitigate gaps identified in the CAP
r) MS Project Plan completed, and inventory of all materials used.

At the end of the Project, Verizon shall provide all artifacts, materials, and work papers associated with the Project to the County, via a secure means.

4. Documentation to be produced by the County and the County Obligations

4.1 The County shall provide relevant policy documentation addressing or related to their security policy or security controls strategies and approaches. The County shall provide a detailed overview of the County's current and planned security controls program to include roles and responsibilities, processes implementing security controls, and any technologies support security controls implementation. The County shall provide the results from any related internal or external security assessments. The County shall ensure access to personnel that support providing security controls. The County shall provide adequate workspace with Internet access and telephone with conferencing capability for the use of the Verizon team.

4.2 Verizon intends to conduct this assessment with its team onsite in Riverside County, from 8am (PST) to 4:30pm (PST), Monday through Friday (excluding County holidays). Verizon's PM, Principal, and Data Manager shall work both onsite and remotely to oversee and manage this Project.

5. Additional Conditions

5.1 Both parties understand and agree that Verizon will not provide County with legal advice or services hereunder. County is responsible for making any determinations as to the sufficiency of County's security program relative to County's OCR audit protocols, including, but not limited to, corrected or uncorrected gaps that may remain the County's security program following Verizon's delivery of the reports required herein.

5.2 County shall inform Verizon of any and all changes to County's project schedule or operating environment that would have a material impact on County's ability to complete the project. The County shall provide and ensure access to personal and information in a timely fashion to allow the assessment processes to stay on schedule.

5.3 County is, and will continue to be, solely responsible for establishing and maintaining internal controls and for complying with applicable laws and regulations.

5.4 County shall remain responsible for the implementation of any recommendations made by Verizon during the course of this project and within Verizon's documentations and deliverables.

5.5 Verizon cannot warrant the work performed by County or County's third party vendors as a provider of consulting services only, without control or responsibility for the County's activities, Verizon cannot be responsible for these situations. Verizon shall rely, without verification, on representations as to the business processes and product capabilities made by County's personnel or those of County's software and hardware vendors and any other third parties.

5.6 Due to the complexities associated with regulatory compliance, Verizon does not, and will not, represent, warrant or provide any assurances that County's business processes and systems or any other business processes and systems (including, without limitation, the business processes and systems of County's vendors, service providers, the County's, unconsolidated subsidiaries or joint ventures in which County has an investment, or other third parties) are compliant with laws and regulations, like HIPAA, or that County's plans, or the plans of any third parties to deal with regulatory or legal compliance, like HIPAA, are sufficient to address and correct any regulatory compliance problems that may arise, or with respect to any other matters relating to regulatory compliance.

5.7 Verizon shall not perform any management functions, make management decisions, or perform in a capacity equivalent to that of an employee of County. In addition, Verizon will not be providing any legal advice or conducting a legal review of any of County's documents, records, or policies.

5.8 County acknowledges and agrees that Verizon will not be responsible (i) for the accuracy or completeness of any information made available by County to Verizon.

5.9 County acknowledges that County is, and will continue to be, solely responsible for establishing and maintaining an effective system of internal control over County's regulatory compliance, including, without limitation, systems designed to assure achievement of its control objectives and its compliance with applicable laws and regulations.

5.10 County shall be solely responsible for, among other things: (a) making all management decisions and performing all management functions; (b) designating a competent management member to oversee the services; (c) evaluating the adequacy and results of the services; (d) accepting responsibility for the results of the services; (e) any and all regulatory compliance and (f) establishing and maintaining internal controls, including, without limitation, monitoring ongoing activities.

5.11 It is understood and agreed that Verizon's services may include advice and recommendations, but all decisions in connection with the implementation of such advice and recommendations shall be the sole responsibility of, and made by, County. In connection with its services hereunder, Verizon shall be entitled to rely on all decisions and approvals of County.

Exhibit B
Payment Provisions

Fixed Price and Milestone Payments

The fixed price for the professional services in this Agreement is $830,000.00 payable in four milestones as follows:

Milestone 1: $166,000.00 upon full execution of the Agreement.
Milestone 2: $249,000.00 upon Findings Review presentation to County management.
Milestone 3: $249,000.00 upon delivery of Draft Reports and discussion with County management.
Milestone 4: $166,000.00 delivery of Final Reports as described in Exhibit A to include on-site County management presentation.

The services provided herein may be subject to taxes, which will be billed separately on the invoice, and which the County will pay.

For additional professional services beyond the scope of this Agreement, the following rates shall apply:

Resource Type	Rate/Hour
Principal Consultant	$245
Senior Consultant	$215
Project Manager	$185

Expenses

Subject to compliance with County's normal and customary policies of business expenses, Verizon is authorized to incur customary and reasonable travel, lodging, and other associated expenses in connection with the performance of the professional services in this Agreement. Verizon may invoice these expenses monthly in arrears; the County will reimburse Verizon for those expenses. Notwithstanding the foregoing, travel expenses shall not exceed eighty three thousand dollars ($83,000.00) or ten percent (10%) of the fixed price.

Exhibit C

COUNTY OF RIVERSIDE
INFORMATION SECURITY OFFICE

The Information Security Requirements stated in this Exhibit are applicable to Verizon's work under this Agreement

1. Health Insurance Portability and Accountability Act (HIPAA) - Privacy, Security, and Breach Notification Rules
2. U.S. Department of Health and Human Services Title 45 C.F.R. Parts 160 and 164
3. Health Information Technology for Economic and Clinical Health (HITECH) Act - Enforcement Rule
4. U.S. Department of Health and Human Services Title 45 C.F.R. Parts 160 and 164
5. California Confidentiality of Medical Information Act
6. California Civil Code § 56
7. California Public Records Act
8. California Government Code §§ 6250-6276.48
9. California Security Breach Notification Law
10. California Civil Code §§ 1798.29 and 1798.82
11. California Trusted System Laws
12. California Government Code § 12168.7
13. California Code of Regulations Title 2 §§ 22620.1-8
14. Riverside County Records Management and Archives Policy
15. Riverside County Board of Supervisors Policy A-43
16. Riverside County Electronic Media and Use Policy
17. Riverside County Board of Supervisors Policy A-50
18. Riverside County Information Security Policy
19. Riverside County Board of Supervisors Policy A-58
20. Riverside County Trustworthy Official Electronic Records Preservation Policy
21. Riverside County Board of Supervisors Policy A-68
22. Riverside County Health Privacy and Security Policy
23. Riverside County Board of Supervisors Policy B-23

1 AUTHORITY

The Riverside County Information Security Requirements (Requirements) was developed in accordance with Board of Supervisors Policy A-58 and has been approved for countywide use by the Chief Information Security Officer (CISO) acting as a representative of the Riverside County Board of Supervisors. Violations of the Requirements may result in immediate disqualification from procurement actions or immediate removal from County networks and other potentially affected information technology resources.

2 PURPOSE AND SCOPE

The Requirements defines the minimum security controls required for securing County information, including the systems, technologies, and processes, through which information is acquired, created, processed, stored, transmitted, and destroyed.
County employees, business associates, Verizon's, vendors, and other non-County employees with direct or indirect access to County information (Users) shall be required to read, understand, and comply with the Requirements and any applicable Specification(s).
Questions regarding these Requirements may be directed to the Information Security Office.

3 ROLES AND RESPONSIBILITIES

3.1 Department Information Security Officer

The Department Information Security Officer (DISO) shall be responsible for ensuring that requirements defined herein are integrated into their respective department's procurement policies and that all software and services meet these requirements. The DISO shall further be responsible for the reporting and remediation of any gaps and deficiencies identified during the course of business based on the Requirements.

3.2 Information Security Office

The Information Security Office (ISO) shall be responsible for assisting each DISO with the implementation of, and ongoing compliance with the Requirements.

4 REQUIREMENTS

4.1 Account and Access Management

Named accounts must be used, generic account use is prohibited.
Accounts for terminated or transferred employees shall be disabled or removed on the day of termination or transfer.
Service-level and system-level accounts may not be directly used by administrators or users for logging on to a system, installing software, or performing changes to a system.
Access to information shall be restricted to user groups unless individual access to information is explicitly required by their role within the organization.

4.1.1 Account and Screen Lockout/Device Wipe

(a) Servers, Workstations, and Online Services

Accounts must be configurable to automatically lock after a predetermined number of consecutive failed logon attempts.
Systems shall be configured such that the screen is automatically locked after a period of inactivity and on resume, display the logon screen after:
User accounts must be configurable to remain locked for a predetermined amount of time or until they are unlocked by an administrator.
Administrative, privileged, and service-level and system-level accounts must be configurable so that whenever they become locked for any reason they shall remain locked until an administrator unlocks them.

(b) Mobile Devices

Devices shall be configurable so that they are automatically wiped (sanitized) after a predetermined number of consecutive failed logon attempts.
Devices shall feature the ability to be remotely wiped (sanitized).
Devices shall be configurable to automatically lock after a predetermined duration of inactivity.

4.1.2 Account Review

Default (vendor supplied) accounts shall be renamed, disabled, or removed. If these accounts cannot be disabled or removed for business or technical reasons, the password shall be changed from the default to conform to the password requirement as defined herein.

4.1.3 Authentication

At a minimum, accounts shall require a username and password for authentication.

(a) Access to secured County information from the Internet shall require multi-factor authentication.

(b) A minimum of two authentication factors shall be used which may include:

(c) Something a user knows, such as a password or a personal identification number (PIN);

(d) Something a user is, including biometrics such as a fingerprint, retinal scan, or facial recognition; or

(e) Something a user physically possesses, such as a smart card, a hardware or software authentication token, a mobile device, or an individually assigned and revocable certificate.

4.2 Anti-Malware

County Requirements and ISO approved anti-malware solutions shall be installed, centrally managed, and maintained on the following:

(a) Servers and Workstations
(b) Mobile Devices

4.3 Computer Kiosks/Public Terminals

Specific requirements for these systems shall be issued on a case-by-case basis by the ISO. Use of these systems shall be reviewed and approved on an annual basis.

4.4 Device Naming

Internet facing technologies shall use logical DNS names that do not disclose technical information about their installed applications, services, or operating systems.

4.5 Electronic Public Records/Trusted Systems

Systems, technologies, and processes used to acquire, process, store, transmit, or retrieve information which qualifies or has been documented as a "public record" based on a Departmental Records Retention Schedule (DRRS), or in accordance with the California Public Records Act, shall be managed in compliance with the Riverside County Records Management and Archives Policy (Board of Supervisors Policy A-43) and Riverside County Trustworthy Official Electronic Records Preservation Policy (Board of Supervisors Policy A-68).

4.6 Encryption

All devices and media which may be used for storing or transporting County confidential information shall utilize a County-approved storage encryption method or technology.

4.7 Log Management

At a minimum, the following controls shall be available for configuration:

4.7.1 Log management systems must be able to audit and log the following activities:

4.7.2 System Events

(a) Active and imminent hardware failures (e.g., low disk space)
(b) Software installations and uninstallations (includes patches and updates)
(c) Started and stopped processes, services and daemons
(d) User, group, and computer account creations, modifications, and deletions

4.7.3 Security Events

a) Successful and failed authentication attempts
b) Anti-virus events (e.g., definition updates, malware infections, removal, and quarantine)
c) Host and network-based firewall, IDS, and IPS events (e.g., DoS, brute force, P2P, reconnaissance, anomalous traffic, correlated events)

4.7.4 Network Events

a) DNS, DHCP, and NTP events
b) Firewall, router and switch events (i.e., informational and above)

4.7.5 Application Events

a) Database events
b) Mission-critical application events
c) Web server events (e.g., Apache, IIS logs)

4.7.6 All logged events shall:

a) reflect accurate date and time stamps
b) be restricted to only authorized administrators and ISO members

c) be retained for a minimum of ninety (90) days

4.7.7 For systems containing Confidential and/or Highly Available information, logs shall:

a) be retained on a dedicated log management server

b) be reviewed on a quarterly basis

4.7.8 Password history limitations are not required.

4.8 Time Synchronization

All technologies, wherever possible, shall be configured such that their clocks are automatically synchronized with the time provided by RCIT's network time protocol (NTP) servers.

4.9 Public Cloud

Public Cloud is the preferred Cloud Computing Platform to leverage for non-sensitive/regulated information to reside upon lower performance applications and bulk data storage. It is a mid to long term goal to move more production services into the Public Cloud; testing and development systems which are not using production data may be good candidates for near term migration. When utilizing Public Cloud, the provider shall adhere to the following:

a) Service provider shall meet all County Board of Supervisors policy requirements

b) Provider's data center and all replicated data shall reside in the United States

c) Provider's data center shall meet Statement on Standards for Attestation Engagements (SSAE) 16 Type II requirements or equivalent

d) All connectivity between the provider and County networks shall be encrypted

e) All backup tapes or other off-site storage of sensitive County information shall be encrypted

f) Any confidential/sensitive data shall be encrypted at-rest

g) External networks and systems hosting sensitive County information shall meet (at a minimum) all requirements defined within the County Information Security Standard

h) The provider shall use individual Microsoft Active Directory (or individual LDAP) accounts when logging in directly, no generic account use for individuals; service accounts may be specified where necessary for programmatic access. These accounts shall adhere to all password requirements set forth in the Information Security Standard. Accounts shall be able to be centrally managed by county staff. Personal accounts may not be used for County purposes

i) All application access on both the County side and the provider side shall be audited and be made available upon request

j) Provider Service Level Agreement (SLA) and privacy policy shall meet all requirements of the County relevant to the information or service(s) involved

k) Application, system, and data isolation shall meet all requirements of the County in relation to the information or service(s) involved

l) Data disposal shall meet County requirements

m) Provider shall provide incident response procedures for review by ISO

n) Provider shall provide any existing risk assessments, internal security policies (to include HIPAA if applicable)

o) Service shall support eDiscovery and records retention (Board of Supervisors Policies A-43 and A-68) requirements wherever applicable

p) Data ownership is retained by the County

q) Background checks are necessary for all of the providers' staff that may have access to County information

r) If Protected Health Information is to be hosted on the Public Cloud, the service provider shall sign the County Board of Supervisors approved Business Associate Agreement as well as adhering to all aforementioned requirements

4.10 Policy References:

a) Riverside County Health Privacy and Security Policy (BOS Policy B-23)
b) Riverside County Records Management and Archives Policy (BOS Policy A-43)
c) Riverside County Electronic Media and Use Policy (BOS Policy A-50)
d) Riverside County Enterprise Information Systems Security Policy (BOS Policy A-58)
e) Riverside County Trustworthy Official Electronic Records Preservation Policy (BOS Policy A-68)
f) Riverside County Information Security Requirements
g) Revision History

Exhibit D, Confidential Information

(To be delivered to Verizon at initial kick off meeting)

As part of this project, County will provide to Verizon certain confidential information that is to be used by Verizon as part of its work for this Agreement only.

Exhibit E, Forms

HIPAA COW

RISK ANALYSIS & RISK MANAGEMENT TOOLKIT NETWORKING GROUP

SUMMARY OF RISK ASSESSMENT STEPS – NIST SP 800-30

The purpose of this document is to provide a high level summary of the nine risk assessment steps outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems* (NIST SP 800-30). A copy of the NIST SP 800-30 flowchart of the steps is on page 3.

General Risk Assessment Overview

Risk assessments can be completed by using many different methodologies. There is no single methodology that will work for all organizations and all situations. The following steps represent key steps to complete a comprehensive risk assessment program as outlined in NIST SP 800-30. These steps should be customized to most effectively identify risks for an organization based on its own uniqueness. Even though these items are listed as steps, they are not prescriptive in the order that they should be conducted. Some steps can be conducted simultaneously rather than sequentially.

Step 1. System Characterization

The first step in assessing risk is to define the scope of the effort. To do this, identify where ePHI is created, received, maintained, processed, or transmitted. Using information-gathering techniques, the IT system boundaries are identified, as well as the resources and the information that constitute the system. Take into consideration policies, laws, the remote work force and telecommuters, and removable media and portable computing devices (e.g., laptops, removable media, and backup media). *Output* – Characterization of the IT system assessed, a good picture of the IT system environment, and delineation of system boundary.

Step 2. Threat Identification

For this step, potential threats (the potential for threat-sources to successfully exercise a particular vulnerability) are identified and documented. A threat-source is any circumstance or event with the potential to cause harm to an IT system (intentional or unintentional). Common threat-sources can be natural, human, or environmental (refer to the Threat Source List for examples). Consider all potential threat-sources; review of historical incidents and data from intelligence agencies, the government, etc., help generate items to place on the list. Tailor the list based on the individual organization and its

processing environment. *Output* – A threat statement containing a list of threat-sources that could exploit system vulnerabilities.

Step 3. Vulnerability Identification

The goal of this step is to develop a list of technical and non-technical system vulnerabilities (flaws or weaknesses) that could be exploited or triggered by the potential threat-sources. Vulnerabilities can range from incomplete or conflicting policies that govern an organization's computer usage to insufficient safeguards to protect facilities that house computer equipment to any number of software, hardware, or other deficiencies that comprise an organization's computer network. *Output* – A list of the system vulnerabilities (observations) that could be exercised by the potential threat-sources.

Step 4. Control Analysis

The goal of this step is to document and assess the effectiveness of technical and non-technical controls that have been or will be implemented by the organization to minimize or eliminate the likelihood (or probability) of a threat-source exploiting a system vulnerability. *Output* – List of current or planned controls (policies, procedures, training, technical mechanisms, insurance, etc.) used for the IT system to mitigate the likelihood of a vulnerability being exercised and reduce the impact of such an adverse event.

Step 5. Likelihood Determination

The goal of this step is to determine the overall likelihood rating that indicates the probability that a vulnerability could be exploited by a threat-source given the existing or planned security controls. *Output* – Likelihood rating of low (.1), medium (.5), or high (1). Refer to the NIST SP 800-30 definitions of low, medium, and high.

Step 6. Impact Analysis

The goal of this step is to determine the level of adverse impact that would result from a threat successfully exploiting a vulnerability. Factors of the data and systems to consider should include the importance to the organization's mission; sensitivity and criticality (value or importance); costs associated; loss of confidentiality, integrity, and availability of systems and data. *Output* – Magnitude of impact rating of low (10), medium (50), or high (100). Refer to the NIST SP 800-30 definitions of low, medium, and high.

Step 7. Risk Determination

By multiplying the ratings from the likelihood determination and impact analysis, a risk level is determined. This represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk rating also presents actions that senior management (the mission owners) must take for each risk level. *Output* – Risk level of low (1-10), medium (>10-50) or high (>50-100). Refer to the NIST SP 800-30 definitions of low, medium, and high.

Step 8. Control Recommendations

The purpose of this step is to identify controls that could reduce or eliminate the identified risks, as appropriate to the organization's operations. The goal of these controls is to reduce the level of risk to the system and data to an acceptable level. Factors to consider when developing controls may include effectiveness of recommended options (i.e., system compatibility), legislation and regulation, organizational policy, operational impact, and safety and reliability. Control recommendations provide input to the risk mitigation process, during which the recommended procedural and technical security

controls are evaluated, prioritized, and implemented. *Output* – Recommendation of control(s) and alternative solutions to mitigate risk.

Step 9. Results Documentation

Results of the risk assessment are documented in an official report or briefing and provided to senior management (the mission owners) to make decisions on policy, procedure, budget, and system operational and management changes. *Output* – A risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation.

After completing this nine-step risk assessment process, the next step is risk mitigation. Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process.

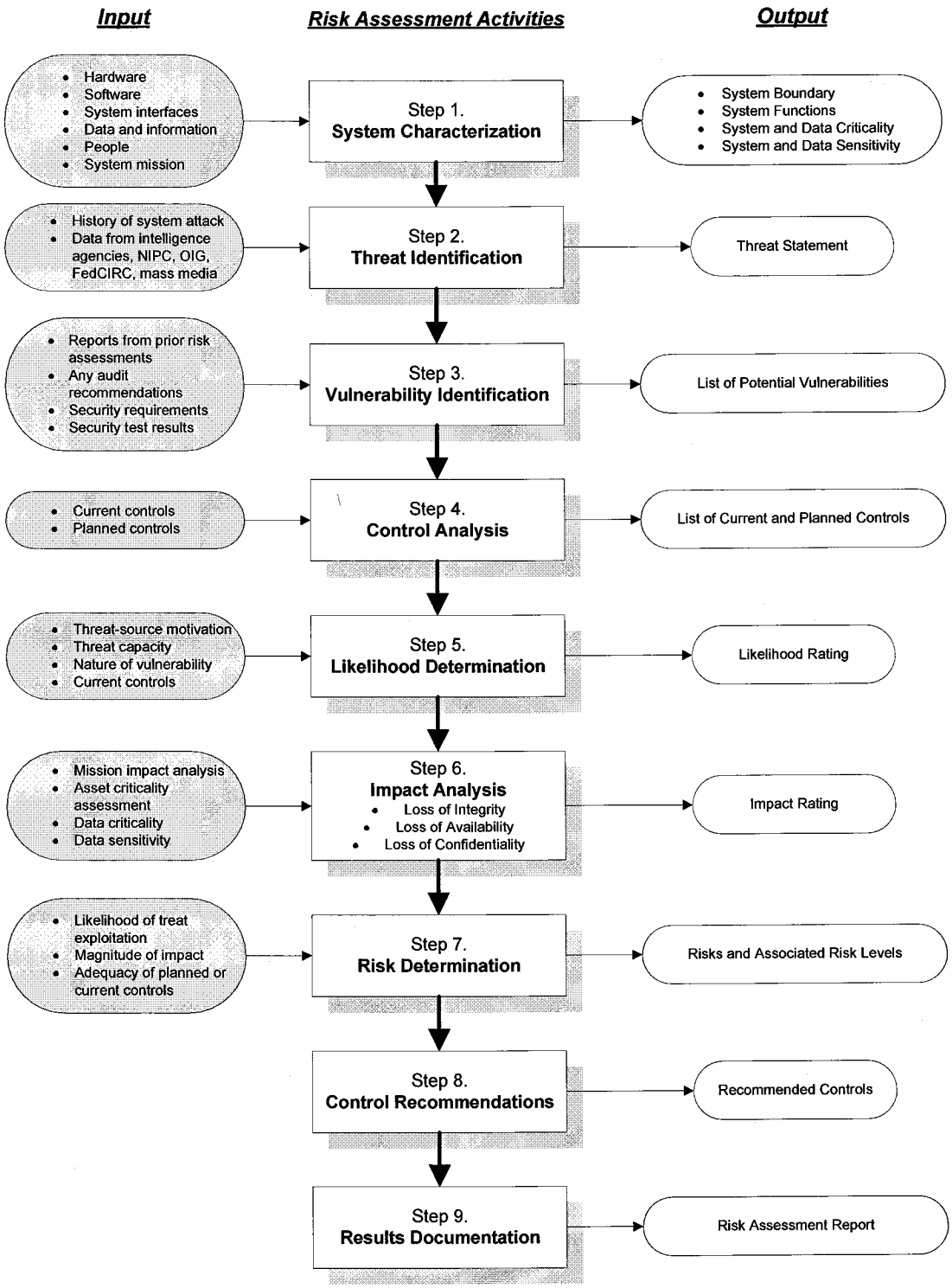
Primary Author: Holly Schlenvogt, MSH, CPM, Health Information Technology Specialist and Privacy & Security Lead, MetaStar/WHITEC

Contributing Authors: HIPAA COW Risk Analysis & Risk Management Toolkit Networking Group Members:

- Kathy Argall, Co-Founder and CEO, InfoSec Compliance Advisors
- Cathy Boerner, JD, CHC, President, Boerner Consulting, LLC
- Ginny Gerlach, Information Security Officer, Ascension Health
- Lee Kadel, MMOT, EMBA, GHSC, GSEC, Information Security Analyst – Specialist, Wheaton Franciscan Healthcare
- Jim Sehloff, MS, MT(ASCP), Information Security Analyst, CareTech Solutions
- Kirsten Wild, RN, BSN, MBA, CHC, Wild Consulting, Inc.

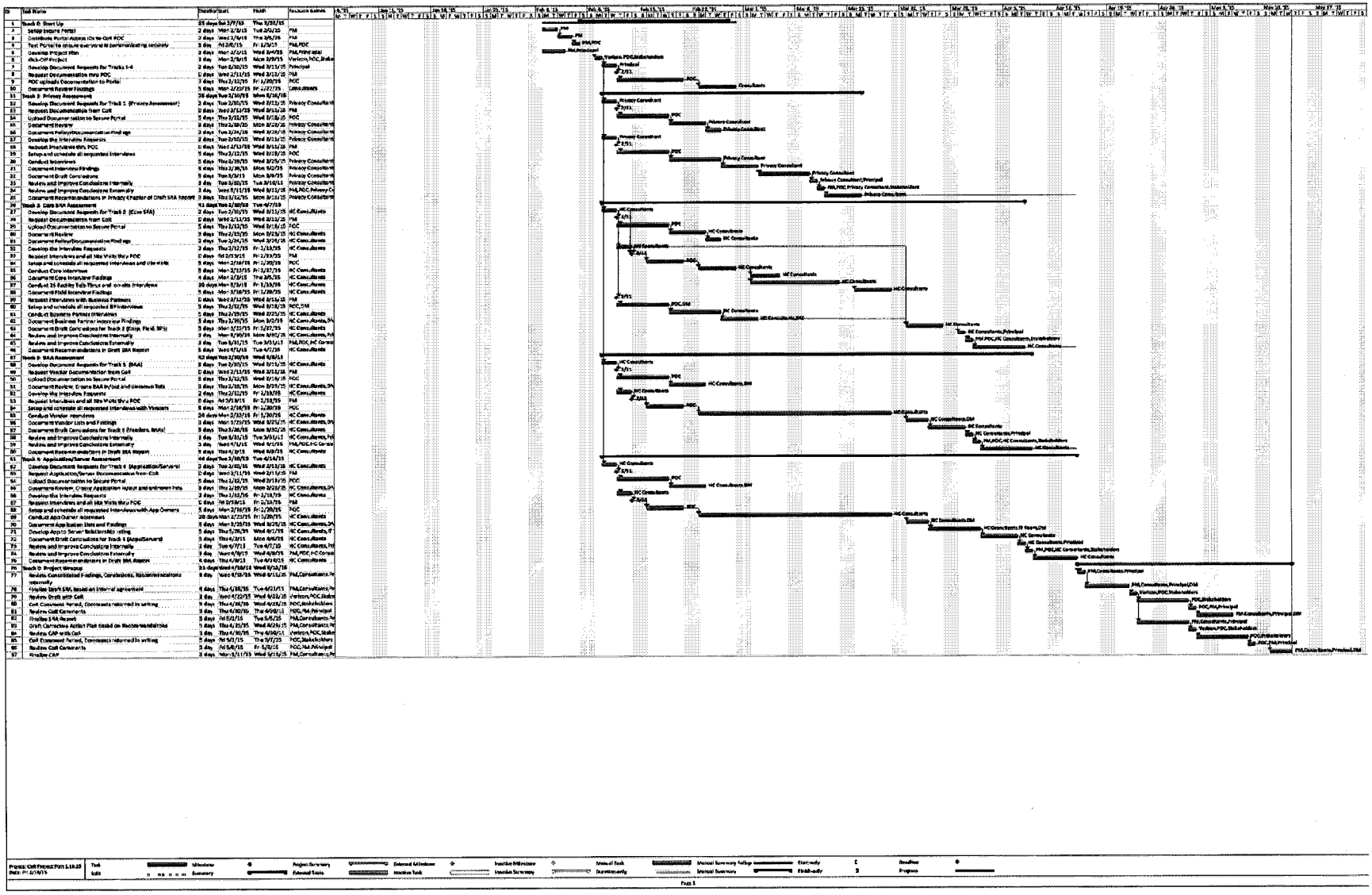
Risk Assessment Methodology Flowchart

NIST SP 800-30



This flowchart was taken directly from NIST SP 800-30

Exhibit F, High Level Project Plan



Attachment I

HIPAA Business Associate Agreement
Addendum to Contract
Between the County of Riverside and Verizon Business Services

This HIPAA Business Associate Agreement (the "Addendum") supplements, and is made part of the Comprehensive HIPAA Security Risk Analysis (the "Underlying Agreement") between the County of Riverside ("County") and Verizon Business Network Services Inc., on behalf of MCI Communications Services, Inc. dba Verizon Business Services ("Verizon") and shall be effective as of the date the Underlying Agreement is signed by both Parties (the "Effective Date").

RECITALS

WHEREAS, County and Verizon entered into the Underlying Agreement pursuant to which the Verizon provides services to County, and in conjunction with the provision of such services certain protected health information ("PHI") and/or certain electronic protected health information ("ePHI") may be created by or made available to Verizon for the purposes of carrying out its obligations under the Underlying Agreement; and,

WHEREAS, the provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Public Law 104-191 enacted August 21, 1996, and the Health Information Technology for Economic and Clinical Health Act ("HITECH") of the American Recovery and Reinvestment Act of 2009, Public Law 111-5 enacted February 17, 2009, and the laws and regulations promulgated subsequent thereto, as may be amended from time to time, are applicable to the protection of any use or disclosure of PHI and/or ePHI pursuant to the Underlying Agreement; and,

WHEREAS, County is a covered entity, as defined in the Privacy Rule; and,

WHEREAS, to the extent County discloses PHI and/or ePHI to Verizon or Verizon creates, receives, maintains, transmits, or has access to PHI and/or ePHI of County, Verizon is a business associate, as defined in the Privacy Rule; and,

WHEREAS, pursuant to 42 USC §17931 and §17934, certain provisions of the Security Rule and Privacy Rule apply to a business associate of a covered entity in the same manner that they apply to the covered entity, the additional security and privacy requirements of HITECH are applicable to business associates and must be incorporated into the business associate agreement, and a business associate is liable for civil and criminal penalties for failure to comply with these security and/or privacy provisions; and,

WHEREAS, the parties mutually agree that any use or disclosure of PHI and/or ePHI must be in compliance with the Privacy Rule, Security Rule, HIPAA, HITECH and any other applicable law; and,

WHEREAS, the parties intend to enter into this Addendum to address the requirements and obligations set forth in the Privacy Rule, Security Rule, HITECH and HIPAA as they apply to Verizon as a business associate of County, including the establishment of permitted and required uses and disclosures of PHI and/or ePHI created or received by Verizon during the course of performing functions, services and activities on behalf of County, and appropriate limitations and conditions on such uses and disclosures;

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

1. **Definitions.** Terms used, but not otherwise defined, in this Addendum shall have the same meaning as those terms in HITECH, HIPAA, Security Rule and/or Privacy Rule, as may be amended from time to time.

   A. "Breach" when used in connection with PHI means the acquisition, access, use or disclosure of PHI in a manner not permitted under subpart E of the Privacy Rule which compromises the security or privacy of the PHI, and shall have the meaning given such term in 45 CFR §164.402.

      (1) Except as provided below in Paragraph (2) of this definition, acquisition, access, use, or disclosure of PHI in a manner not permitted by subpart E of the Privacy Rule is presumed to be a breach unless Verizon demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following four factors:

(a) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

(b) The unauthorized person who used the PHI or to whom the disclosure was made;

(c) Whether the PHI was actually acquired or viewed; and

(d) The extent to which the risk to the PHI has been mitigated.

(2) Breach excludes:

(a) Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of the Privacy Rule.

(b) Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity, business associate, or organized health care arrangement in which County participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted by subpart E of the Privacy Rule.

(c) A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

B. "Business associate" has the meaning given such term in 45 CFR §164.501, including but not limited to a subcontractor that creates, receives, maintains, transmits or accesses PHI on behalf of the business associate.

C. "Data aggregation" has the meaning given such term in 45 CFR §164.501.

D. "Designated record set" as defined in 45 CFR §164.501 means a group of records maintained by or for a covered entity that may include: the medical records and billing records about individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or, used, in whole or in part, by or for the covered entity to make decisions about individuals.

E. "Electronic protected health information" ("ePHI") as defined in 45 CFR §160.103 means protected health information transmitted by or maintained in electronic media.

F. "Electronic health record" means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff, and shall have the meaning given such term in 42 USC §17921(5).

G. "Health care operations" has the meaning given such term in 45 CFR §164.501.

H. "Individual" as defined in 45 CFR §160.103 means the person who is the subject of protected health information.

I. "Person" as defined in 45 CFR §160.103 means a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private.

J. "Privacy Rule" means the HIPAA regulations codified at 45 CFR Parts 160 and 164, Subparts A and E.

K. "Protected health information" ("PHI") has the meaning given such term in 45 CFR §160.103, which includes ePHI.

L. "Required by law" has the meaning given such term in 45 CFR §164.103.

M. "Secretary" means the Secretary of the U.S. Department of Health and Human Services ("HHS").

N. "Security incident" as defined in 45 CFR §164.304 means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

O. "Security Rule" means the HIPAA Regulations codified at 45 CFR Parts 160 and 164, Subparts A and C.

P. "Subcontractor" as defined in 45 CFR §160.103 means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

Q. "Unsecured protected health information" and "unsecured PHI" as defined in 45 CFR §164.402 means PHI not rendered unusable, unreadable, or indecipherable to unauthorized persons through use of a technology or methodology specified by the Secretary in the guidance issued under 42 USC §17932(h)(2).

2. **Scope of Use and Disclosure by Verizon of County's PHI and/or ePHI.**

A. Except as otherwise provided in this Addendum, Verizon may use, disclose, or access PHI and/or ePHI as necessary to perform any and all obligations of Verizon under the Underlying Agreement or to perform functions, activities or services for, or on behalf of, County as specified in this Addendum, if such use or disclosure does not violate HIPAA, HITECH, the Privacy Rule and/or Security Rule.

B. Unless otherwise limited herein, in addition to any other uses and/or disclosures permitted or authorized by this Addendum or required by law, in accordance with 45 CFR §164.504(e)(2), Verizon may:

1) Use PHI and/or ePHI if necessary for Verizon's proper management and administration and to carry out its legal responsibilities; and,

2) Disclose PHI and/or ePHI for the purpose of Verizon's proper management and administration or to carry out its legal responsibilities, only if:

a) The disclosure is required by law; or,

b) Verizon obtains reasonable assurances, in writing, from the person to whom Verizon will disclose such PHI and/or ePHI that the person will:

i. Hold such PHI and/or ePHI in confidence and use or further disclose it only for the purpose for which Verizon disclosed it to the person, or as required by law; and,

ii. Notify County of any instances of which it becomes aware in which the confidentiality of the information has been breached; and,

3) Use PHI to provide data aggregation services relating to the health care operations of County pursuant to the Underlying Agreement or as requested by County; and,

4) De-identify all PHI and/or ePHI of County received by Verizon under this Addendum provided that the de-identification conforms to the requirements of the Privacy Rule and/or Security Rule and does not preclude timely payment and/or claims processing and receipt.

C. Notwithstanding the foregoing, in any instance where applicable state and/or federal laws and/or regulations are more stringent in their requirements than the provisions of HIPAA, including, but not limited to, prohibiting disclosure of mental health and/or substance abuse records, the applicable state and/or federal laws and/or regulations shall control the disclosure of records.

3. **Prohibited Uses and Disclosures.**

A. Verizon may neither use, disclose, nor access PHI and/or ePHI in a manner not authorized by the Underlying Agreement or this Addendum without patient authorization or de-identification of the PHI and/or ePHI and as authorized in writing from County.

B. Verizon may neither use, disclose, nor access PHI and/or ePHI it receives from County or from another business associate of County, except as permitted or required by this Addendum, or as required by law.

C. Verizon agrees not to make any disclosure of PHI and/or ePHI that County would be prohibited from making.

D. Verizon shall not use or disclose PHI for any purpose prohibited by the Privacy Rule, Security Rule, HIPAA and/or HITECH, including, but not limited to 42 USC §17935 and §17936. Verizon agrees:

1) Not to use or disclose PHI for fundraising , unless pursuant to the Underlying Agreement and only if permitted by and in compliance with the requirements of 45 CFR §164.514(f) or 45 CFR §164.508;

2) Not to use or disclose PHI for marketing, as defined in 45 CFR §164.501, unless pursuant to the Underlying Agreement and only if permitted by and in compliance with the requirements of 45 CFR §164.508(a)(3);

3) Not to disclose PHI, except as otherwise required by law, to a health plan for purposes of carrying out payment or health care operations, if the individual has requested this restriction pursuant to 42 USC §17935(a) and 45 CFR §164.522, and has paid out of pocket in full for the health care item or service to which the PHI solely relates; and,

4) Not to receive, directly or indirectly, remuneration in exchange for PHI, or engage in any act that would constitute a sale of PHI, as defined in 45 CFR §164.502(a)(5)(ii), unless permitted by the Underlying Agreement and in compliance with the requirements of a valid authorization under 45 CFR §164.508(a)(4). This prohibition shall not apply to payment by County to Verizon for services provided pursuant to the Underlying Agreement.

4. **Obligations of County.**

A. County agrees to make its best efforts to notify Verizon promptly in writing of any restrictions on the use or disclosure of PHI and/or ePHI agreed to by County that may affect Verizon's ability to perform its obligations under the Underlying Agreement, or this Addendum.

B. County agrees to make its best efforts to promptly notify Verizon in writing of any changes in, or revocation of, permission by any individual to use or disclose PHI and/or ePHI, if such changes or revocation may affect Verizon's ability to perform its obligations under the Underlying Agreement, or this Addendum.

C. County agrees to make its best efforts to promptly notify Verizon in writing of any known limitation(s) in its notice of privacy practices to the extent that such limitation may affect Verizon's use or disclosure of PHI and/or ePHI.

D. County agrees not to request Verizon to use or disclose PHI and/or ePHI in any manner that would not be permissible under HITECH, HIPAA, the Privacy Rule, and/or Security Rule.

E. County agrees to obtain any authorizations necessary for the use or disclosure of PHI and/or ePHI, so that Verizon can perform its obligations under this Addendum and/or Underlying Agreement.

5. **Obligations of Verizon.** In connection with the use or disclosure of PHI and/or ePHI, Verizon agrees to:

A. Use or disclose PHI only if such use or disclosure complies with each applicable requirement of 45 CFR §164.504(e). Verizon shall also comply with the additional privacy requirements that are applicable to covered entities in HITECH, as may be amended from time to time.

B. Not use or further disclose PHI and/or ePHI other than as permitted or required by this Addendum or as required by law. Verizon shall promptly notify County if Verizon is required by law to disclose PHI and/or ePHI.

C. Use appropriate safeguards and comply, where applicable, with the Security Rule with respect to ePHI, to prevent use or disclosure of PHI and/or ePHI other than as provided for by this Addendum.

D. Mitigate, to the extent practicable, any harmful effect that is known to Verizon of a use or disclosure of PHI and/or ePHI by Verizon in violation of this Addendum.

E. Report to County any use or disclosure of PHI and/or ePHI not provided for by this Addendum or otherwise in violation of HITECH, HIPAA, the Privacy Rule, and/or Security Rule of which Verizon becomes aware, including breaches of unsecured PHI as required by 45 CFR §164.410.

F. In accordance with 45 CFR §164.502(e)(1)(ii), require that any subcontractor that create, receive, maintain, transmit or access PHI on behalf of the Verizon agree through contract to the same restrictions and conditions that apply to Verizon with respect to such PHI and/or ePHI, including the restrictions and conditions pursuant to this Addendum.

G. Make available to County or the Secretary, in the time and manner designated by County or Secretary, Verizon's internal practices, books and records relating to the use, disclosure and privacy protection of PHI received from County, or created or received by Verizon on behalf of County, for purposes of determining, investigating or auditing Verizon's and/or County's compliance with the Privacy Rule.

H. Request, use or disclose only the minimum amount of PHI necessary to accomplish the intended purpose of the request, use or disclosure in accordance with 42 USC §17935(b) and 45 CFR §164.502(b)(1).

I. Comply with requirements of satisfactory assurances under 45 CFR §164.512 relating to notice or qualified protective order in response to a third party's subpoena, discovery request, or other lawful process for the disclosure of PHI, which Verizon shall promptly notify County upon Verizon's receipt of such request from a third party.

J. Not require an individual to provide patient authorization for use or disclosure of PHI as a condition for treatment, payment, enrollment in any health plan (including the health plan administered by County), or eligibility of benefits, unless otherwise excepted under 45 CFR §164.508(b)(4) and authorized in writing by County.

K. Use appropriate administrative, technical and physical safeguards to prevent inappropriate use, disclosure, or access of PHI and/or ePHI.

L. Obtain and maintain knowledge of applicable laws and regulations related to HIPAA and HITECH, as may be amended from time to time.

M. Comply with the requirements of the Privacy Rule that apply to the County to the extent Verizon is to carry out County's obligations under the Privacy Rule.

N. Take reasonable steps to cure or end any pattern of activity or practice of its subcontractors of which Verizon becomes aware that constitute a material breach or violation of the subcontractor's obligations under the business associate contract with Verizon, and if such steps are unsuccessful, Verizon agrees to terminate its contract with the subcontractor if feasible.

6. **Access to PHI, Amendment and Disclosure Accounting.** Verizon agrees to:

A. **Access to PHI, including ePHI.** Provide access to PHI, including ePHI if maintained electronically, in a designated record set to County or an individual as directed by County, within five (5) days of request from County, to satisfy the requirements of 45 CFR §164.524.

B. **Amendment of PHI.** Make PHI available for amendment and incorporate amendments to PHI in a designated record set County directs or agrees to at the request of an individual, within fifteen (15) days of receiving a written request from County, in accordance with 45 CFR §164.526.

C. **Accounting of disclosures of PHI and electronic health record.** Assist County to fulfill its obligations to provide accounting of disclosures of PHI under 45 CFR §164.528 and, where applicable, electronic health records under 42 USC §17935(c) if Verizon uses or maintains electronic health records. Verizon shall:

1) Document such disclosures of PHI and/or electronic health records, 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 and/or electronic health record in accordance with 45 CFR §164.528.

2) Within fifteen (15) days of receiving a written request from County, provide to County or any individual as directed by County information collected in accordance with this section to permit County to respond to a request by an individual for an accounting of disclosures of PHI and/or electronic health record.

3) Make available for County information required by this Section 6.C for six (6) years preceding the individual's request for accounting of disclosures of PHI, and for three (3) years preceding the individual's request for accounting of disclosures of electronic health record.

7. **Security of ePHI.** In the event County discloses ePHI to Verizon or Verizon needs to create, receive, maintain, transmit or have access to County ePHI, in accordance with 42 USC §17931 and 45 CFR §164.314(a)(2)(i), and §164.306, Verizon shall:

1. Comply with the applicable requirements of the Security Rule, and implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI that Verizon creates, receives, maintains, or transmits on behalf of County in accordance with 45 CFR §164.308, §164.310, and §164.312;

2. Comply with each of the requirements of 45 CFR §164.316 relating to the implementation of policies, procedures and documentation requirements with respect to ePHI;

3. Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI;

4. Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required under the Privacy Rule;

5. Ensure compliance with the Security Rule by Verizon's workforce;

6. In accordance with 45 CFR §164.308(b)(2), require that any subcontractor that create, receive, maintain, transmit, or access ePHI on behalf of Verizon agree through contract to the same restrictions and requirements contained in this Addendum and comply with the applicable requirements of the Security Rule;

7. Report to County any security incident of which Verizon becomes aware, including breaches of unsecured PHI as required by 45 CFR §164.410; and,

8. Comply with any additional security requirements that are applicable to covered entities in Title 42 (Public Health and Welfare) of the United States Code, as may be amended from time to time, including but not limited to HITECH.

8. **Breach of Unsecured PHI.** In the case of breach of unsecured PHI, Verizon shall comply with the applicable provisions of 42 USC §17932 and 45 CFR Part 164, Subpart D, including but not limited to 45 CFR §164.410.

A. **Discovery and notification.** Following the discovery of a breach of unsecured PHI, Verizon shall notify County in writing of such breach without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, except as provided in 45 CFR §164.412.

1) **Breaches treated as discovered.** A breach is treated as discovered by Verizon as of the first day on which such breach is known to Verizon or, by exercising reasonable diligence, would have been known to Verizon, which includes any person, other than the person committing the breach, who is an employee, officer, or other agent of Verizon (determined in accordance with the federal common law of agency).

2) **Content of notification.** The written notification to County relating to breach of unsecured PHI shall include, to the extent possible, the following information if known (or can be reasonably obtained) by Verizon:

a) The identification of each individual whose unsecured PHI has been, or is reasonably believed by Verizon to have been accessed, acquired, used or disclosed during the breach;

b) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

c) A description of the types of unsecured PHI involved in the breach, such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved;

d) Any steps individuals should take to protect themselves from potential harm resulting from the breach;

e) A brief description of what Verizon is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and,

f) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, web site, or postal address.

B. **Cooperation.** With respect to any breach of unsecured PHI reported by Verizon, Verizon shall cooperate with County and shall provide County with any information requested by County to enable County to fulfill in a timely manner its own reporting and notification obligations, including but not limited to providing notice to individuals, prominent media outlets and the Secretary in accordance with 42 USC §17932 and 45 CFR §164.404, §164.406 and §164.408.

C. **Breach log.** To the extent breach of unsecured PHI involves less than 500 individuals, Verizon shall maintain a log or other documentation of such breaches and provide such log or other documentation on an annual basis to County not later than fifteen (15) days after the end of each calendar year for submission to the Secretary.

D. **Delay of notification authorized by law enforcement.** If Verizon delays notification of breach of unsecured PHI pursuant to a law enforcement official's statement that required notification, notice or posting would impede a criminal investigation or cause damage to national security, Verizon shall maintain documentation sufficient to demonstrate its compliance with the requirements of 45 CFR §164.412.

E. **Payment of costs.** With respect to any breach of unsecured PHI caused solely by the Verizon's failure to comply with one or more of its obligations under this Addendum and/or the provisions of HITECH, HIPAA, the Privacy Rule or the Security Rule, Verizon agrees to pay any and all costs associated with providing all legally required notifications to individuals, media outlets, and the Secretary. This provision shall not be construed to limit or diminish Verizon's obligations to indemnify, defend and hold harmless County under Section 9 of this Addendum.

F. **Documentation.** Pursuant to 45 CFR §164.414(b), in the event Verizon's use or disclosure of PHI and/or ePHI violates the Privacy Rule, Verizon shall maintain documentation sufficient to demonstrate that all notifications were made by Verizon as required by 45 CFR Part 164, Subpart D, or that such use or disclosure did not constitute a breach, including Verizon's completed risk assessment and investigation documentation.

G. **Additional State Reporting Requirements.** The parties agree that this Section 8.G applies only if and/or when County, in its capacity as a licensed clinic, health facility, home health agency, or hospice, is required to report unlawful or unauthorized access, use, or disclosure of medical information under the more stringent requirements of California Health & Safety Code §1280.15. For purposes of this Section 8.G, "unauthorized" has the meaning given such term in California Health & Safety Code §1280.15(j)(2).

1) Verizon agrees to assist County to fulfill its reporting obligations to affected patients and to the California Department of Public Health ("CDPH") in a timely manner under the California Health & Safety Code §1280.15.

2) Verizon agrees to report to County any unlawful or unauthorized access, use, or disclosure of patient's medical information without unreasonable delay and no later than two (2) business days after Verizon

detects such incident. Verizon further agrees such report shall be made in writing, and shall include substantially the same types of information listed above in Section 8.A.2 (Content of Notification) as applicable to the unlawful or unauthorized access, use, or disclosure as defined above in this section, understanding and acknowledging that the term "breach" as used in Section 8.A.2 does not apply to California Health & Safety Code §1280.15.

9. **Hold Harmless/Indemnification.**

A. Verizon agrees to indemnify and hold harmless County, all Agencies, Districts, Special Districts and Departments of County, their respective directors, officers, Board of Supervisors, elected and appointed officials, employees, agents and representatives from any liability whatsoever, based or asserted upon any services of Verizon, its officers, employees, subcontractors, agents or representatives arising out of or in any way relating to this Addendum, including but not limited to property damage, bodily injury, death, or any other element of any kind or nature whatsoever arising from the performance of Verizon, its officers, agents, employees, subcontractors, agents or representatives from this Addendum. Verizon shall defend, at its sole expense, all costs and fees, including but not limited to attorney fees, cost of investigation, defense and settlements or awards, of County, all Agencies, Districts, Special Districts and Departments of County, their respective directors, officers, Board of Supervisors, elected and appointed officials, employees, agents or representatives in any claim or action based upon such alleged acts or omissions.

B. With respect to any action or claim subject to indemnification herein by Verizon, Verizon shall, at their sole cost, have the right to use counsel of their choice, subject to the approval of County, which shall not be unreasonably withheld, and shall have the right to adjust, settle, or compromise any such action or claim without the prior consent of County; provided, however, that any such adjustment, settlement or compromise in no manner whatsoever limits or circumscribes Verizon's indemnification to County as set forth herein. Verizon's obligation to defend, indemnify and hold harmless County shall be subject to County having given Verizon written notice within a reasonable period of time of the claim or of the commencement of the related action, as the case may be, and information and reasonable assistance, at Verizon's expense, for the defense or settlement thereof. Verizon's obligation hereunder shall be satisfied when Verizon has provided to County the appropriate form of dismissal relieving County from any liability for the action or claim involved.

C. The specified insurance limits required in the Underlying Agreement of this Addendum shall in no way limit or circumscribe Verizon's obligations to indemnify and hold harmless County herein from third party claims arising from issues of this Addendum.

D. In the event there is conflict between this clause and California Civil Code §2782, this clause shall be interpreted to comply with Civil Code §2782. Such interpretation shall not relieve the Verizon from indemnifying County to the fullest extent allowed by law.

E. In the event there is a conflict between this indemnification clause and an indemnification clause contained in the Underlying Agreement of this Addendum, this indemnification shall only apply to the subject issues included within this Addendum.

10. **Term.** This Addendum shall commence upon the Effective Date and shall terminate when all PHI and/or ePHI provided by County to Verizon, or created or received by Verizon on behalf of County, is destroyed or returned to County, or, if it is infeasible to return or destroy PHI and/ePHI, protections are extended to such information, in accordance with section 11.B of this Addendum.

11. **Termination.**

A. **Termination for Breach of Contract.** A breach of any provision of this Addendum by either party shall constitute a material breach of the Underlying Agreement and will provide grounds for terminating this Addendum and the Underlying Agreement with or without an opportunity to cure the breach, notwithstanding any provision in the Underlying Agreement to the contrary. Either party, upon written notice to the other party describing the breach, may take any of the following actions:

1) Terminate the Underlying Agreement and this Addendum, effective immediately, if the other party breaches a material provision of this Addendum.

2) Provide the other party with an opportunity to cure the alleged material breach and in the event the other party fails to cure the breach to the satisfaction of the non-breaching party in a timely manner, the non-breaching party has the right to immediately terminate the Underlying Agreement and this Addendum.

3) If termination of the Underlying Agreement is not feasible, the breaching party, upon the request of the non-breaching party, shall implement, at its own expense, a plan to cure the breach and report regularly on its compliance with such plan to the non-breaching party.

B. **Effect of Termination.**

1) Upon termination of this Addendum, for any reason, Verizon shall return or, if agreed to in writing by County, destroy all PHI and/or ePHI received from County, or created or received by the Verizon on behalf of County, and, in the event of destruction, Verizon shall certify such destruction, in writing, to County. This provision shall apply to all PHI and/or ePHI which are in the possession of subcontractor or agents of Verizon. Verizon shall retain no copies of PHI and/or ePHI, except as provided below in paragraph (2) of this section.

2) In the event that Verizon determines that returning or destroying the PHI and/or ePHI is not feasible, Verizon shall provide written notification to County of the conditions that make such return or destruction not feasible. Upon determination by Verizon that return or destruction of PHI and/or ePHI is not feasible, Verizon shall extend the protections of this Addendum to such PHI and/or ePHI and limit further uses and disclosures of such PHI and/or ePHI to those purposes which make the return or destruction not feasible, for so long as Verizon maintains such PHI and/or ePHI.

12. **General Provisions.**

A. **Retention Period.** Whenever Verizon is required to document or maintain documentation pursuant to the terms of this Addendum, Verizon shall retain such documentation for 6 years from the date of its creation or as otherwise prescribed by law, whichever is later.

B. **Amendment.** The parties agree to take such action as is necessary to amend this Addendum from time to time as is necessary for County to comply with HITECH, the Privacy Rule, Security Rule, and HIPAA generally.

C. **Survival.** The obligations of Verizon under Sections 3, 5, 6, 7, 8, 9, 11.B and 12.A of this Addendum shall survive the termination or expiration of this Addendum.

D. **Regulatory and Statutory References.** A reference in this Addendum to a section in HITECH, HIPAA, the Privacy Rule and/or Security Rule means the section(s) as in effect or as amended.

E. **Conflicts.** The provisions of this Addendum shall prevail over any provisions in the Underlying Agreement that conflict or appear inconsistent with any provision in this Addendum.

F. **Interpretation of Addendum.**

1) This Addendum shall be construed to be part of the Underlying Agreement as one document. The purpose is to supplement the Underlying Agreement to include the requirements of the Privacy Rule, Security Rule, HIPAA and HITECH.

2) Any ambiguity between this Addendum and the Underlying Agreement shall be resolved to permit County to comply with the Privacy Rule, Security Rule, HIPAA and HITECH generally.

G. **Notices to County.** All notifications required to be given by Verizon to County pursuant to the terms of this Addendum shall be made in writing and delivered to the County both by fax and to both of the addresses listed below by either registered or certified mail return receipt requested or guaranteed overnight mail with tracing capability, or at such other address as County may hereafter designate. All notices to County provided by Verizon pursuant to this Section shall be deemed given or made when received by County.

County HIPAA Privacy Officer:	HIPAA Privacy Manager
County HIPAA Privacy Officer Address:	P.O. Box 1569 Riverside, CA 92502
County HIPAA Privacy Officer Fax Number:	(951) 955-HIPAA or (951) 955-4472

———————— TO BE COMPLETED BY COUNTY PERSONNEL ONLY ————————

County Departmental Officer: _____

County Departmental Officer Title: _____

County Department Address: _____

County Department Fax Number: _____