SUBMITTAL TO THE RIVERSIDE UNIVERSITY HEALTH SYSTEM MEDICAL CENTER GOVERNING BOARD COUNTY OF RIVERSIDE, STATE OF CALIFORNIA

Riverside University HEALTH SYSTEM Medical Center

ITEM 15.1 (ID # 8638)

MEETING DATE:
Tuesday, March 12, 2019

FROM : RUHS-MEDICAL CENTER:

SUBJECT: RIVERSIDE UNIVERSITY HEALTH SYSTEM (RUHS) Approval of the Master Purchase Agreement and MPS Order Form for Monitoring Services between the County of Riverside and Fair Warning Services, LLC, Without Seeking Competitive Bids. All Districts [Total Cost $94,576; up to $9,4576 in additional compensation – 100% Hospital Enterprise Fund. Enterprise Fund]

RECOMMENDED MOTION: That the Board of Supervisors:

1. Approve the Master Purchase Agreement, MPS Order Form and Business Associate Agreement ("Agreement") with Fair Warning Services, LLC, without seeking competitive bids for sixteen months March 12, 2019 through July 27, 2020, not to exceed $94,576.00 and authorize the Chairman of the Board to sign the Agreement on behalf of the County; and
2. Authorize the Purchasing Agent, in accordance with Ordinance No. 459, based on the availability of fiscal funding and as approved by County Counsel to: a) sign amendments that do not change the substantive terms of the agreement and b) sign amendments to the compensation provisions that do not exceed the sum total of ten (10) percent of the total annual cost of the contract.

ACTION:Policy

Jennifer Cruikshank, Chief Executive Officer – Health System 2/19/2019

MINUTES OF THE GOVERNING BOARD

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

Ayes:	Jeffries, Spiegel, Washington, Perez and Hewitt
Nays:	None
Absent:	None
Date:	March 12, 2019
xc:	RUHS-Medical Center, Purchasing

Kecia Harper
Clerk of the Board
By: Deputy

SUBMITTAL TO THE RIVERSIDE UNIVERSITY HEALTH SYSTEM MEDICAL CENTER GOVERNING BOARD OF DIRECTORS COUNTY OF RIVERSIDE, STATE OF CALIFORNIA

FINANCIAL DATA	Current Fiscal Year:	Next Fiscal Year:	Total Cost:	Ongoing Cost
COST	$17,733	$ 70,932	$ 94,576	$ 0
NET COUNTY COST	$ 0	$ 0	$ 0	$ 0
SOURCE OF FUNDS: Hospital Enterprise Fund 40050			Budget Adjustment: No	
			For Fiscal Year: 18/19/-20/21	

C.E.O. RECOMMENDATION: Approve

BACKGROUND:

Summary

The Riverside University Health System (RUHS) seeks to improve its compliance services by proactively addressing risks posed by unauthorized access to electronic medical records. Stemming from the HIPAA Privacy Rule that limits disclosure of health information to the minimum necessary for treatment, payment or operations, RUHS has a policy of providing its workforce access to patient protected health information based on a need-to-know to perform their job duties at RUHS. To monitor workforce access to the EPIC system, RUHS-Corporate Compliance utilizes the Fair Warning software that performs regular access checks and sends automated alerts when certain criteria are met.

As a member of the Loma Linda University Shared Services EHR Platform, RUHS has an obligation to monitor access to the EPIC system. RUHS has ongoing access to Fair Warning's monitoring services as an affiliate of Loma Linda University Medical Center (LLU). Under the proposed contract, RUHS will remain a Loma Linda University (LLU) affiliate, but will gain administrative control over the automated alerts. While Loma Linda University will still host and manage the software licenses, RUHS will be able to select and manage its alerts, separate from Loma Linda University giving RUHS greater flexibility over its resources and more control over the types of alerts received (applying filters for false positives or expanding the criteria).

Impact on Residents and Businesses

Fair Warning will flag and alert RUHS Compliance staff of potential HIPAA violations occurring in the EPIC patient system within the hospital. This monitoring system ensures patient privacy remains a priority and is continuously protected.

Additional Fiscal Information		Year One	Year Two
Year 1	Implementation	$10,800.00	
Year 1	Monitoring	$16,750.67	
Year 2	Monitoring		$67,048.00
Total (each year)		$27,528.00	$67,048.00

The contract is for a 16 month term with the option to renew. The contract provides up to eight enforceable policies (automated alerts). In the first year, RUHS may enforce up to four core enforced polices. Implementation of the four core enforced polices will cost $10,800 in the first year. The implementation includes working with Fair Warning analysts to select the areas deemed essential to the success of the Patient Privacy Monitoring Program with improvement and updates as desired. Fair Warning will customize the alert trigger criteria to meet the needs of RUHS. The monitoring of the contract for the first year, covering the four core enforced policies, will complete the total of $27,528.

The second year will allow RUHS to select an addition four enforced polices, bringing the total of monitored policies to eight. The contracted fee to monitor the eight policies is $67,048,

Because LLU hosts the software, there are no additional fees and no ongoing operational commitment for the County. The total cost of the contract for two years is $94,576.

Contract History and Price Reasonableness

To be a part of the Loma Linda University Shared Services and a Care Connect Partner, RUHS must use the same electronic health record monitoring system as the other entities in the partnership. This contract will allow existing services to continue and provide for additional services all under the control of RUHS while not having to bear the cost of hosting or managing the vendor's software onsite.

ATTACHMENT C. Master Purchase Agreement and MPS Order Form

Teresa Summers, Director of Purchasing 2/19/2019

FAIRWARNING.

ORDER FORM for FairWarning Services, LLC
Order Form No.: RUHS.MPS-OF-7.16.2018
Offer Valid through: 3/12/2019
Proposed by: Nate Kuslanski
Order Form Type: Managed Privacy Services
Quote Number: RUHS.MPS-OF-7.16.2018

MPS Order Form for LLUH Non-Affiliates

ORDER FORM

Prepared for:

Satellite Customer:	The County of Riverside, a political subdivision of the State of California on behalf of Riverside University Health System
Name:	Lekisha Reese, Compliance and Privacy Officer
Address:	26520 Cactus Ave.
City/State/Zip	Moreno Valley, CA 92555
Phone:	951-486-5065
Email:	l.reese@ruhealth.org

Bill to:	The County of Riverside
Address:	26520 Cactus Ave
City/State/Zip:	Moreno Valley, CA 92555
Billing Company Name:	The County of Riverside – RUHS Medical Center
Billing Contact Name:	Lekisha Reese, Compliance and Privacy Officer
Billing Email Address:	l.rrese@ruhealth.org
Billing Phone:	951-486-5065

Terms and Conditions

Related Master Contract:	FairWarning Master Purchase Agreement US_V3.3_(LLUH 2017) ("MPA"), as amended in Section V.A.2) below.
Billing Frequency:	Annual
Billing Method:	Email
Payment Method:	Check
Payment Terms:	Net 45. Annual fees begin on Contract Effective Date with subsequent annual payments due on the anniversary of that date each year thereafter. See implementation services terms referenced elsewhere in this Order Form.
Contract Effective Date:	March 12, 2019 ("Contract Effective Date").
Contract End Date:	July 27, 2020

I. Purchased Services

Summary: Yearly Sub-totals

Year 1 sub-total:	$27,528.00
Year 2 sub-total:	$67,048.00
Grand Total:	$94,576.00

Product Details

Product	Description	Order Term (Years)	Yearly/ Unit Price+	Proration (if applicable)	QTY	Total Price
Subscription Services						
FW-MGDSVC-IMP-B	Managed Privacy Services implementation	n/a	$10,800.00	n/a	1	$10,800.00
FW-MGDSVC-B-YR1	Managed Privacy Services - monitoring	1	$7.39	4 months	6,800	$16,750.67
FW-MGDSVC-B-YR 2	Managed Privacy Services - monitoring	1	$9.86	n/a	6,800	$67,048.00

MAR 12 2019 15.1

II. Services Schedule and Detail

	Year 1	Year 2
Implementation and professional services (First year invoiced upon Contract Effective Date with annual payments due each year thereafter)		
Implementation services (Foundation phase) includes: – Review policies covering select subject areas deemed essential to the success of the Patient Privacy Monitoring Program with suggestions for improvement/updates – Establishment of the following (where applicable): o Standardized workflows o Proven validation process o Communication and education plan o Customized communication and education materials o Guidance on documentation of decisions around the deployment of FairWarning Patient Privacy Monitoring	$10,080.00	
Patient Privacy Monitoring services include: – Implement up to 4 core enforced policies (automated alerts) over the first 12 months of the Initial Term at the suggested rate of 1 enforced policy every 10 - 13 weeks or another schedule mutually agreed upon. – After the initial 4 enforced policies have been implemented, additional enforced policies selected from a menu of available enforced policies may be implemented at the suggested rate of 1 in every 6 months or another schedule mutually agreed upon up to a total of eight (8) enforced policies. The additional enforced policies to be implemented shall be agreed upon in advance and in writing. – Apply specific filters to the enforced policies where applicable and available to reduce the number of false positives. – Provide continuous patient privacy monitoring of the Satellite Customer's applications being supplied to FairWarning® Patient Privacy Monitoring technology through the use of enforced policies (automated alerts) implemented by the FairWarning® Managed Privacy Services staff. – Review of triggered enforced policies by FairWarning® Managed Privacy Services staff in accordance with Service Level Agreements (SLAs) as attached to this Order Form as Exhibit A. – Validate Satellite Customer computer user's access from triggered enforced policies if a business reason cannot be determined. – Documentation of reviews and investigations of triggered enforced policies in FairWarning® Patient Privacy Monitoring technology. – In accordance with SLAs, promptly notify Satellite Customer's designated contact personnel upon discovery of suspected inappropriate access by Satellite Customer computer user. – Provide assistance with access reviews based on complaints (upon request by Satellite Customer) – Provide or assist Satellite Customer with governance and compliance effectiveness reporting. – Provide trending results of positive findings (confirmed inappropriate access) from triggered enforced policies. – Provide recommendations to the Satellite Customer on staff education and awareness initiatives.	$16,750.67	$67,048.00
Total – All Managed Services	$27,528.00	$67,048.00

Prices shown above do not include any taxes that may apply. Any such taxes are the responsibility of Satellite Customer. This is not an invoice. If Satellite Customer is a tax-exempt organization, Satellite Customer must supply FairWarning with a valid tax exemption certificate authorized by the appropriate taxing authority as outlined in section 4.6 of the Master Purchase Agreement.

III. Required information

Base Statistics – Satellite Customer represents and warrants the accuracy of the following facts for Satellite Customer as of the Contract Effective Date of this Order Form:

Number of Monitored Users: 6,800

Satellite Customer contacts for escalation path described in Other Considerations section:

Name/Title (#1) Lekisha Reese

Name /Title (#2) _____

Primary facility for which the Services shall be used

Name RUHS – Medical Center

Address 26520 Cactus Ave

City/state/zip Moreno Valley, CA 92555

Notices should be sent to the following:

Name Lekisha Reese

Address 26520 Cactus Ave

City/state/zip Moreno Valley, CA 92555

Contact Name: _____ Title _____

Email: _____ Phone _____

IV. Term & Renewal

A. The initial term of the items included in Purchased Services shall commence on the Contract Effective Date (as defined on page one above) and end on July 27, 2020, so that it is co-terminous with the initial term or renewal term then in effect for MPS Subscription Services for the "Sponsoring Customer"—as that term is defined and utilized in Section V (Contract Special Terms) below (the "Initial Term"). Unless either party notifies the other in writing of non-renewal at least thirty (30) days prior to expiration of the term, and provided that Sponsoring Customer's software license for the FairWarning patient privacy intelligence solution continues in good standing, the Initial Term may be renewed for successive additional terms (each a "Renewal Term") upon written agreement upon the expiration of the Initial Term and each Renewal Term. Upon any expiration or termination of this Order Form or the MPA, the provisions of Section 10.5 of the MPA shall apply.

V. Contract Special Terms

A. **Satellite Customer Entity & Sponsoring Customer**

1) Customer Entities. As used herein, "Satellite Customer" means the County of Riverside, and shall include the following healthcare provider facilities:

- Riverside University Health Systems

For clarity, the Satellite Customer named in this subparagraph (and referred to in throughout this Order Form) is referred to in the MPA as "You" (*see* definition of "You" or "Your" on page 2 of the MPA and is a "Non-Affiliate" in Sponsoring Customer's MPS Order Form.

2) Purpose. Satellite Customer is entering into a direct contractual relationship with FairWarning Services, LLC ("FairWarning") for the above-identified Purchased Services, subject to the terms and conditions of the MPA. FairWarning and Satellite Customer agree, however, the following amendments shall be effective for the MPA as applied to Satellite Customer ("COUNTY" for the purposes of this subsection A.2) specifically the MPS Services:

> COUNTY's responsibility under MPA Section 3.3 (Your Responsibilities), subsection (b), for "the accuracy, quality and legality of [COUNTY's] Data and the means by which [COUNTY] acquired [COUNTY's] Data" is limited to the extent that COUNTY has control over such "Data."

3) Sponsoring Customer & Precondition. Satellite Customer is also either concurrently entering or has previously entered into a written agreement ("EHR Hosting Agreement") with Loma Linda University Health ("Sponsoring Customer"), a non-affiliated, third party, who is both a customer of FairWarning and a service-provider of software hosting services for (a) at least one Electronic Health Record ("EHR") software application ("Shared EHR Application") for Satellite Customer and other third-party entities not affiliated with Sponsoring Customer ("Other Non-Affiliates") and (b) the FairWarning patient privacy intelligence solution("PPI Solution"). As a

precondition to receiving the above Purchased Services, Sponsoring Customer must have previously entered (or be concurrently entering) into a purchase order agreement ("Data Source Order Form") with FairWarning for the software data source license(s) necessary to deliver both (i) Satellite Customer's event audit log data from Sponsoring Customer's hosted instance of the Shared EHR Application and (ii) Satellite Customer's authoritative user data, (combined, "Satellite Customer Data") to the FairWarning solution.

4) Satellite Customer's Use of Sponsoring Customer's Software License. As part of Sponsoring Customer's Data Source Order Form, FairWarning, LLC—a sister-Affiliate of FairWarning under 100% common ownership—("FairWarning Software Co.")—has agreed to expand the scope of "Permitted Users"—as that term is defined under Section 1 (Definitions) of the MPA—under Sponsoring Customer's software license to include Satellite Customer's Permitted Users. Customer and FairWarning Software Co. have also agreed that Satellite Customer is also an intended third-party beneficiary with regards to (a) the software license granted to, (b) the software hosting platform provided to, and (c) the associated ancillary support and maintenance services provided to Sponsoring Entity under the Data Source Order Form. For clarity, however, and despite not being in direct privity of contract with FairWarning Software Co. for the software license, Satellite Customer's access to and use of Sponsoring Entity's software license, whether for the purpose of receiving the Purchased Services or otherwise, is subject to the terms and conditions of the MPA, including but not limited to MPA Sections 3 (Use of Services), 5 (Proprietary Rights and Licenses), 6 (Confidentiality), and 8 (Mutual Indemnification).

B. **Valid Software License Requirement**. For Satellite Customer to receive the above Purchased Services and derive the intended value, Sponsoring Customer's valid license to use the FairWarning® Licensed Software must be maintained in good standing throughout the entirety of all terms of this Order Form (whether an Initial Term or a Renewal Term). This MPS Order Form shall automatically terminate simultaneous with any termination of Sponsoring Customer's software license with FairWarning Software Co. If Sponsoring Customer's software license is terminated as a result of the act or omission of FairWarning or FairWarning Software Co. (and through no fault of Satellite Customer and no fault of Sponsoring Customer), then Satellite Customer may terminate this MPS Order Form for cause as prescribed in Section 10.3 of the MPA and FairWarning will issue a refund of all prepaid but unused fees paid for monitoring services, pro-rated as of the termination effective date.

C. **Compliance with Laws.** Each party agrees that in furnishing or receiving the Purchased Services offered above, that it (and its Affiliates (as that term is defined in the MPA), agents, subcontractors, and Permitted Users) will materially comply at all times with all applicable local, state, and federal laws, regulations and rules relating thereto.

D. **Shared Data Source Applications and Responsibility for Data Extraction**.

1) Shared EHR Applications and Data Monitoring. As referenced in subsection A.3. above, under the EHR Hosting Agreement(s), Sponsoring Customer is or will be managing significant EHR and IT resources for on behalf of Satellite Customer as well as for other entities who are also third party non-affiliates of Sponsoring Customer ("Other Non-Affiliates"). Under this Order Form and other Order Forms issued to Sponsoring Customer and Other Non-Affiliates; Satellite Customer, Sponsoring Customer, and the Other Non-Affiliates will all have access to the above Purchased Services for the purpose of monitoring their own data (Satellite "Customer Data" and "Other Non-Affiliate Data," respectively), which are subsets of the term "Your Data" as defined in the MPA), which Sponsoring Customer delivers to the FairWarning PPI Solution.

2) Separate Data. Satellite Customer's Data originates from Satellite Customer's authoritative user data and from event audit log data generated by the Shared EHR Application pursuant to Satellite Customer's delivery of healthcare services to its patients at Satellite Customer's facilities. Data for Sponsoring Customer and each of the Other Non-Affiliates likewise originates from their authoritative user data and from event audit log data generated by the Shared EHR Application pursuant to their delivery of healthcare services to their patients at their own facilities. Satellite Customer acknowledges that Sponsoring Customer will be extracting Satellite Customer's data from the Shared EHR Application and delivering that data to a specific file location, from which FairWarning will apply its data script that will parse the already-separated data file and route Satellite Customer's data to the appropriate FairWarning database location.

3) Hosting and Data Extraction Responsibility. Satellite Customer acknowledges that Sponsoring Customer, who hosts the Shared EHR Application to be monitored, is solely responsible for (1) hosting the PPI Solution and (2) accurately extracting and delivering the data from the Shared EHR Application event audit data logs into separate data source feeds before FairWarning can incorporate such data into the FairWarning solution. FAIRWARNING IS NOT RESPONSIBLE FOR THE ACCURACY OR QUALITY OF THE EXTRACTION AND DELIVERY OF (A) EVENT AUDIT LOG DATA OR (B) AUTHORITATIVE USER DATA IN SEPARATE FILES FOR PRESENTATION/PARSING TO THE FAIRWARNING PATIENT PRIVACY INTELLIGENCE SOLUTION.

E. **Dependency on the Set-Up and Delivery of Data and Controls**. FairWarning's ability to separately provide the Purchased Services, including the analytics and reports that may be available, and to separately monitor Satellite Customer's Data apart from Sponsoring Customer's data (and from the Data of Other Non-Affiliates) is significantly dependent upon (a) the structural set-up and continued delivery of the Shared EHR Application event audit log data and authoritative user data from the applicable third-party software applications, whether

independent or shared, to the FairWarning PPI Solution, and (b) the User access controls and credentialing, which will be issued and activated exclusively by the system administrators for Sponsoring Customer, Satellite Customer, and each of the Other Non-Affiliates, but not by FairWarning. FAIRWARNING SHALL NOT BE RESPONSIBLE THE ACTS OR OMISSIONS OF SPONSORING CUSTOMER, SATELLITE CUSTOMER, OR ANY OTHER NON-AFFILIATE OR THEIR RESPECTIVE WORKFORCES IN (1) HOSTING OR ACCESSING THE FAIRWARNING PPI SOLUTION (2) ISSUING OR MAINTAINING USER ACCESS AND CREDENTIALING CONTROLS FOR THE FAIRWARINING PPI SOLUTION, OR (3) RECEIVING THE PURCHASED SERVICES; INCLUDING BUT NOT LIMITED TO ANY SUCH ACTS OR OMISSIONS ASSOCIATED WITH THE ACCURACY, PRIVACY, OR SECURITY OF DATA.

F. **Indemnification of FairWarning**. In addition to the Indemnification Obligations of Section 8 of the MPA, Satellite Customer shall defend and indemnify FairWarning against any loss, liability, damage, cost, or expense (including reasonable attorney fees and litigation costs), arising out of any claims or suits that may be made or brought against FairWarning ("Claim Against FairWarning") arising out of:

(1) Satellite Customer's access to (or use or disclosure) of, (i) Sponsoring Customer Data or (ii) the Data of any Other Non-Affiliate;

(2) The negligent acts or omissions of Satellite Customer or its Workforce in (i) providing inaccurate and/or incorrect guidance and information to FairWarning regarding the structural set up for the delivery of data to the FairWarning PPI Solution, or (ii) issuing or activating the user access controls or credentialing;

(3) Any third-party claim, demand, fine, suit, or proceeding made or brought against FairWarning alleging that Satellite Customer's shared use of the FairWarning PPI Solution, has violated (i) such third party's rights of privacy, intellectual property, or employment, or (ii) any applicable federal or state law;

(4) Any dispute or proceeding arising between Satellite Customer and either Sponsoring Customer or any Other Non-Affiliate(s) related to or arising out of any EHR Hosting Agreement(s) or any other services agreement(s) under which Sponsoring Customer delivers Satellite Customer Data to the FairWarning PPI Solution;

(5) Any claim, demand, fine, suit, or proceeding made or brought against FairWarning by any third party for FairWarning's termination of the Purchased Services based on Sponsoring Customer's failure to (i) maintain the Software License in good standing, (ii) continue to provide Satellite Customer's Data to the FairWarning PPI Solution, or (iii) continue to provide Satellite Customer with sufficient ongoing access to the Purchased Services.

(6) The above indemnifications will not apply to the extent that such Claim Against FairWarning is caused by FairWarning's (1) negligent act or omission, including but not limited to a breach of this Order Form or the MPA, or (2) willful misconduct.

(7) Further, Satellite Customer agrees that it will look directly to Sponsoring Customer and will not bring against FairWarning or FairWarning Software Co. for any claim, demand, fine, suit, or proceeding based on a claim that Sponsoring Customer has failed to (i) maintain the Software License in good standing (other than arising out of Sponsoring Customer's termination of the Software License Services for uncured cause under Section 10.3 of the MPA), (ii) to continue to sufficiently provide Satellite Customer's Data to the FairWarning PPI Solution, or (iii) to continue to provide Satellite Customer with sufficient ongoing access to the Purchased Services.

G. **Indemnification of Satellite Customer.** In addition to FairWarning's defense and indemnification obligations of Section 8.1 (Indemnification by Us) of the MPA for third-party claims alleging a violation of law or infringement or misappropriation of third-party intellectual property, FairWarning shall indemnify and hold harmless also defend Satellite Customer, 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") against any third-party claim, demand, suit or proceeding alleging (1) FairWarning's breach of this Order Form or the MPA or (2) the negligence or willful misconduct in the provision Services under this Order Form by FairWarning, its officers, employees, subcontractors, agents or representatives. For clarity, the same defense and indemnification obligations, rights, and limitations prescribed in Section 8.1 (e.g., right to prompt notice and sole control of the defense, etc.) shall apply to FairWarning's defense and indemnification obligations under this Section V.G, and FairWarning shall indemnify the Indemnitees for all damages, costs and fees (including, but not limited, to reasonable attorney fees, cost of investigation, defense and settlements or awards).

H. **Indemnification Obligation Exemptions and Survival**. Any indemnification obligation arising under the preceding Sections F and G shall not be subject to the limitations and exclusions of MPA Sections 9.1 (Limitation of Liability) or 9.2 (Exclusion of Consequential and Related Damages). Any such indemnification obligation that arises or accrues prior to the expiration or termination of this Order Form, including any renewals, shall survive such expiration or termination.

VI. Common terms used in Managed Privacy Services engagements

- "Access" generally refers to the act of a computer user of the customer (where for purposes of this Section VI only, "customer" shall generally refer to a customer of FW, whether Customer, Sponsoring Customer, or an Other Non-Affiliate) in accessing ePHI within an electronic health record ("EHR") or application(s) maintained by customer.
- "Access Review" refers to the review of customer's computer system user(s) who have accessed a patient's EHR and/or other clinical applications. This may involve identifying all users who accessed the record at issue or identifying whether a specific user accessed the record.
- "Communication Plan" means the communication plan to inform the customer's own employees/workforce of (1) the increased monitoring activities being implemented and (2) what the organizational policies are for acceptable use and unacceptable behavior regarding Access to customer's applications containing ePHI.
- "Enforced Policies" are reports (1) with specific criteria designed to detect specific activities or behavior, (2) that can be scheduled and will automatically alert or "trigger" when that specific criteria is met.
- "Investigation" means examination of customer's computer user's Access to ePHI that was identified as potentially not business related during the review of a triggered Enforced Policy, including documenting in the FairWarning Patient Privacy Monitoring Technology in the "Investigation" area.
- "Special Alert" means an Enforced Policy created for a specific situation or event (e.g., for a high profile patient that is in the hospital).
- "Validation Request" means the written request that FairWarning sends to customer's management personnel after review of a triggered enforced policy, when the review failed to identify a likely business reason for the Access.

VII. Customer Responsibilities

1) Secured VPN Connection - Satellite Customer shall provide a secured VPN connection over the Internet.
2) Satellite Customer shall have established Transport Layer Security ("TLS") for all of the Satellite Customer domains with the domains of FairWarning within 15 days of Contract Effective Date.
3) Provide FairWarning® Managed Privacy Services staff the Satellite Customer's policy(ies) covering the select subject areas identified by the FairWarning Managed Privacy Services staff for review.
4) Work with the FairWarning® Managed Privacy Services staff to identify appropriate Satellite Customer management personal for incorporation into standardized workflows and validation processes.
5) Work with the FairWarning Managed Privacy Services staff to finalize the communications plan for Satellite Customer's organization.
6) Execute and deliver either (a) a communication and education plan (as created by FairWarning® with Satellite Customer's assistance) or (b) a substantially equivalent plan that has been mutually agreed upon in writing after consultation with FairWarning, where FairWarning's agreement will not be unreasonably withheld.
7) Ensure timely line management response to FairWarning's Validation Request in validating suspicious or inappropriate access (within 3 business days) to allow FairWarning to adequate time to meet FairWarning's SLA commitment to complete and document any investigation into inappropriate Access within 5-7 business days.
8) When notified by FairWarning® Managed Privacy Services staff, review and close all documented reviews and investigations of triggered enforced policies. This includes Satellite Customer's sole responsibility for determining if the investigation is a confirmed incident and if it is a reportable Breach under state or federal law.
9) Carry out any required patient and/or government notifications as reasonably determined by Satellite Customer.
10) Carry out appropriate training and sanctions according to Customer's internal policies as indicated by investigations of triggered enforced policies that FairWarning® Managed Privacy Services staff has initiated and Satellite Customer has followed up on and finalized.
11) Follow either (a) the education and awareness initiatives recommended by FairWarning® Managed Privacy Services staff based on FairWarning's knowledge of best practices and the trending of positive findings from FairWarning's review of the triggered enforced policies or (b) substantially equivalent measures mutually agreed upon in writing after consultation with FairWarning on the best practices, where FairWarning's agreement will not be unreasonably withheld.
12) Provide IT support as reasonably required (data feeds, adding additional data fields to extracts, etc.).
13) Other actions reasonably suggested by the FairWarning® team and mutually agreed upon in writing.

VIII. Other Considerations

1) The Managed Privacy Services pricing and resource estimates are based on Satellite Customer follow up on the Investigations initiated and conducted by the FairWarning Managed Privacy Services staff and taking appropriate action with Satellite Customer's employees based on the Satellite Customer's subsequent review and determination for investigations. Therefore, FairWarning expects the Satellite Customer will review, close and carry out, within 2 weeks of receiving FairWarning's hand-off of a Triggered Enforce Policy and/or Investigation needing further Satellite Customer-level review, whatever appropriate follow-up/sanctioning activities may be for the Investigations initiated and performed by FairWarning. If the Satellite Customer does not perform the review and follow-up within such 2-week period, the FairWarning Managed Privacy Services staff will escalate to escalation contact #1 [e.g., Privacy Officer]. After 2 additional weeks if the review and follow-up has not been completed, the issue will be escalated to escalation contact #2 [e.g. Executive Sponsor]. FairWarning reserves the right to consider Satellite Customer's demonstrated pattern of failing to complete the reviews and carry out appropriate (as reasonably determined by Satellite Customer) follow-up/sanctioning for a period of 8 weeks a material breach of the terms of this Order Form and subject to termination under section 10.3 in the Master Purchase Agreement. Any single Investigation not completed and/or closed within the 2-week period for reasonable good cause specific to the details of that Investigation shall not be included in FairWarning's reasonable determination of whether Satellite Customer has demonstrated a pattern of such failures.
2) The monitoring services apply specifically to Access of ePHI by Satellite Customer computer users in possession of valid credentials – i.e., credentials that are issued and activated by the Satellite Customer.
3) Monitoring services only pertain to Satellite Customer's EHR and healthcare applications whose audit logs are being provided to the FairWarning® Privacy Monitoring Technology.
4) Governance and Compliance reports along with trending will be used to monitor all entities' compliance with responsibilities related to this Service.
5) All Enforced Policies may not be available based on the core application (usually an EHR) being monitored.
6) Monitoring is dependent on scheduled delivery of data to the FairWarning® Privacy Monitoring Technology.
7) Assistance with Urgent EHR Investigations (which are not a result of the FairWarning® Managed Privacy Services monitoring) is available for additional charges (The current rate is $250/hr.). Examples of Urgent EHR Investigations include investigations driven by law enforcement activities such as:
    - Investigations into suspected identity theft or fraud activities utilizing patient information
    - Government/Regulatory investigations

IX. Adjustments to Managed Services Fees

The below-identified software subscription fees to be paid annually by Satellite Customer under this Order Form ("Applicable Fees") were quoted and agreed to based in part upon certain assumptions, which are identified as "Base Statistics" above and Satellite Customer represents and warrants the accuracy of the Base Statistics relating to Satellite Customer and its Affiliates as of the Contract Effective Date. Satellite Customer acknowledges and expressly agrees that in the event that the Base Statistics increases or decreases by more than ten percent (10%) during the term of this Order Form (including any Renewal Terms) as determined in accordance with the below methodology and as is prescribed below, (i) FairWarning shall have the right to increase or decrease the Applicable Fees by a corresponding percentage, and (ii) Satellite Customer shall promptly remit payment.

Items included in Applicable Fees:

- FW-MGDSVC-B FairWarning Managed Privacy Services - annual monitoring services

Methodology:

(a) Measurement Dates & Periods: Commencing on the date which is six (6) months after the Contract Effective Date and continuing thereafter in twelve (12) month intervals (each, a "Measurement Date"), FairWarning will review the corresponding Base Statistics data as is then available on Satellite Customer's primary web site and, if necessary, any other publicly-available information sources. For the facilities for which the services and software are provided under this Order Form (the "Purchased Services"), if the then-current value of the Base Statistics has increased by more than ten percent (10%) during the period between the (i) Contract Effective Date and the then-current Measurement Date (the "Term Measurement Period") and (ii) during the period between the preceding Measurement Date and the Measurement Date at issue (the "Interval Measurement Period"), FairWarning shall notify Satellite Customer of the percentage increase for the statistics and provide Satellite Customer with a supplemental invoice that reflects the corresponding percentage increase in the Applicable Fees. If the Measurement Date at issue is the first Measurement Date, then the Interval Measurement Period shall be the Term Measurement Period.

(b) Pricing Adjustments : In the event that any the Base Statistics has increased as of the Measurement Date at issue by more than ten percent (10%) during the Term Measurement Period, then the Applicable Fees to be paid by Satellite Customer for the next annual billing period commencing after the Measurement Date at issue (and each subsequent annual billing period thereafter, unless and until adjusted again pursuant to this provision) shall be increased

to an amount equal to the Applicable Fees in effect at the commencement of the Term increased in proportion to the percentage increase in the Base Statistics during the Term Measurement Period, plus an adjustment for any prior annual increases. FairWarning shall notify Satellite Customer in writing of any increase so calculated within sixty (60) days of the applicable Measurement Date. In the event that the percentage change in the Base Statistics during any Interval Measurement Period is a decrease (the "Decrease") of more than ten percent (10%), then the Applicable Fees to be paid by Satellite Customer for the next annual billing period commencing after the Measurement Date at issue shall be decreased to an amount equal to the Applicable Fees in effect at the commencement of the Interval Measurement Period decreased in proportion to the Decrease; provided, however, that in no event may the Applicable Fees be reduced to an amount which is less than the Applicable Fees in effect at the commencement of the term of this Agreement (i.e., the original Applicable Fees listed above on this Order Form).

(c) Example (for illustrative purposes only, where the Base Statistic in this example is "employees" instead of "Monitored Users"):

(i) If the Contract Effective Date is May 1, 2014, then the first Measurement Date will be November 1, 2014, and another Measurement Date will occur each November 1 thereafter during the term of this Order Form, including any Renewal Terms. For the facilities for which the Purchased Services are provided, if the Base Statistics equal 4,000 employees, and the corresponding statistics for Satellite Customer's use of the Purchased Services on the first Measurement Date equal 4,100, then there shall be no adjustment in the Applicable Fees on the first Measurement Date because the percentage increase over the corresponding Base Statistics during the Term Measurement Period would have been only 100 (or 2.5%) for the number of employees, which is less than 10%.

(ii) If on the second Measurement Date, the corresponding statistics equal 4,480 employees (an increase of 12%, in comparison with the Base Statistics), then the Applicable Fees shall, as of the second Measurement Date, be increased to a total of 112% of what such fees were as of the Contract Effective Date, with such percentage increase remaining in effect until another adjustment (if any) is made in accordance herewith.

(iii) If on the third Measurement Date, the corresponding statistics equal 5,000 employees (an increase of 25%, in comparison with the Base Statistics), then the Applicable Fees shall, as of the third Measurement Date, be increased to a total of 125% of what such fees were as of the Contract Effective Date, with such percentage increase remaining in effect until another adjustment (if any) is made in accordance herewith.

(iv) If on the fourth Measurement Date, the corresponding statistics equal 4,300 (a decrease of 14%, in comparison with the prior Measurement Date), then the Applicable Fees shall, as of the fourth Measurement Date, be decreased by 14% of what such fees were as of the last Measurement Date, with such percentage decrease remaining in effect until another adjustment (if any) is made in accordance herewith.

This Order Form is issued pursuant to and is subject to all terms and conditions of that certain Related Master Agreement referenced above. Satellite Customer acknowledges having reviewed, understands and accepts the Related Master Purchase Agreement expressly identified above and all terms and conditions thereof. Subject to any contrary provisions in that Related Master Agreement and except for the service discontinuation mechanism prescribed in Contract Special Term B above for Managed Providers, subscriptions, licenses, and maintenance and support commitments are non-cancelable before the end of the Initial Term.

COUNTY OF RIVERSIDE, a political subdivision of the State of California, On behalf of Riverside University Health Systems

By: _____

Name: Kevin Jeffries

Title: Chairman, Board of Supervisors

Date: MAR 12 2019

ATTEST: KECIA R. HARPER, Clerk
By: _____ DEPUTY

FORM APPROVED COUNTY COUNSEL
BY: _____ DATE
SYNTHIA M. GUNZEL

FAIRWARNING SERVICES, LLC, a Florida limited liability company

By: _____

Name: Daniel Singer

Title: Vice President & Treasurer

Date: 2/5/19

EXHIBT A - Service Level Agreements

1) Enforced Policies triggered and delivered to the FairWarning solution between 9 am Mon and 12 pm Fri, Eastern Time, will be reviewed within 24 hours.
2) Enforced Policies triggered and delivered to the FairWarning solution between 12 pm Fri and 9 am Mon, Eastern Time, will be reviewed by 5 pm Tuesday.
3) Any Investigations into potential inappropriate Access will be completed and documented by the FairWarning® Managed Services Staff within 5-7 business days, contingent upon Satellite Customer's management response to Validation Request within 3 business days.
4) Notification of Satellite Customer representative by FairWarning® Managed Services Staff upon completion of any Investigations into inappropriate Access.
5) Completion of Access Reviews within 7 business days.
6) In the event of a widespread natural disaster or similar emergency effecting FairWarning® or the Sponsoring or Satellite Customers, SLAs may be negatively impacted.

Holiday Hours: Each year, the below holidays will be exempt (i.e., not included in the calculations) for the response times listed above. The FairWarning MPS team will perform their scheduled review of the alerts the next business day after the holiday. If a holiday falls on a weekend, FairWarning MPS personnel will have either the Friday before or the following Monday off instead. FairWarning will notify Customers in advance each calendar year regarding the exact timing of the holidays being observed.

- New Year's Day
- Memorial Day
- Independence Day
- Labor Day
- Thanksgiving
- Day After Thanksgiving
- Christmas Eve
- Christmas
- New Year's Eve

FAIRWARNING.

Master Purchase Agreement

THE FAIRWARNING GROUP OF AFFILIATED COMPANIES IS THE GLOBAL LEADER IN PATIENT PRIVACY MONITORING FOR ELECTRONIC HEALTH RECORDS. WE PROVIDE PATIENT PRIVACY MONITORING SOLUTIONS THROUGH LICENSES OF OUR PROPRIETARY SOFTWARE, SOFTWARE AS A SERVICE, AND ANCILLARY MANAGED SERVICES. THIS AGREEMENT GOVERNS YOUR ACQUISITION AND USE OF OUR SERVICES FROM ANY FAIRWARNING AFFILIATE AND REGARDLESS OF THE TYPE OF SERVICES YOU PURCHASE.

EACH PARTY EXECUTING AN ORDER FORM THAT REFERENCES AND INCORPORATES THIS AGREEMENT THEREBY ACCEPTS AND AGREES TO THE TERMS OF THIS AGREEMENT. ANY PERSON SIGNING AN ORDER FORM THEREBY REPRESENTS THAT THEY HAVE THE AUTHORITY TO BIND THE ENTITY NAMED IN THE ORDER FORM TO THESE TERMS AND CONDITIONS.

You may not access the Services if You are Our direct competitor, except with Our prior written consent. In addition, You may not access the Services for purposes of monitoring their availability, performance or functionality, or for any other benchmarking or competitive purposes.

This Master Purchase Agreement is entitled "FairWarning Master Purchase Agreement US V3.3 (LLUH – 2017)". It is effective between You and Us as of the last date of signature on the first Order Form executed by You and Us under this Agreement ("Effective Date").

Table of Contents

1. DEFINITIONS

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Agreement**" and/or "**MPA**" means this Master Purchase Agreement.

"**Documentation**" means Our online user guides, documentation, and help and training materials, as updated from time to time, accessible via www.fairwarning.com or login to the applicable Service.

"**Malicious Code**" means code, files, scripts, agents or programs intended to do harm, including, for example, viruses, worms, time bombs and Trojan horses.

"**Order Form**" means an ordering document specifying the Services to be provided hereunder that is entered into between You and Us or any of Our Affiliates, including any addenda and supplements thereto. By entering into an Order Form hereunder, an Affiliate agrees to be bound by the terms of this Agreement as if it were an original party hereto.

"**Permitted Users**" shall mean (i) Users acting under Your control, including outpatient clinics, ambulatory surgical/care centers, ancillary service providers, outreach clients, clinics, non-acute and acute care service, offices of physicians and other caregivers who have privileges at, provide services at, or are affiliated with Your facility; provided, however, that all such Users shall be permitted to use the Services solely in conjunction with the review of information pertaining to their performance of services relating to Your patients at Your facilities, or (ii) as otherwise defined in the applicable Order Form.

"**Purchased Services**" means Services that You or Your Affiliate purchase under an Order Form.

"**Services**" means the products and services that are ordered by You under a free trial or an Order Form and made available by Us, including software, software as a service, appliances, ancillary managed services, and associated offline components, as described in the Documentation.

"**User**" means an individual who is authorized by You to use a Service, for whom You have ordered the Service, and to whom You (or We at Your request) have supplied a user identification and password. Users may include, for example, Your employees, consultants, contractors and agents, and third parties with which You transact business.

"**We**," "**Us**" or "**Our**" means the FairWarning company that accepts this Agreement by signing one or More Order Forms.

"**You**" or "**Your**" means the company or other legal entity which accepts this Agreement by signing one or more Order Forms, and Affiliates of that company or entity that are expressly identified in that Order Form.

"**Your Data**" means electronic data and information submitted by or for You to the Purchased Services or collected and processed by or for You using the Purchased Services.

2. OUR RESPONSIBILITIES

2.1. Provision of Purchased Services. We will (a) make the Services available to You pursuant to this Agreement and the applicable Order Forms, (b) provide Our support for the Purchased Services to You pursuant to the applicable Order Forms, and (c) use commercially reasonable efforts to make the online Purchased Services available 24 hours a day, 7 days a week, except for: (i) planned downtime (of which We shall give at least 8 hours electronic notice and which We shall schedule to the extent practicable during the weekend hours between 6:00 p.m. Friday and 3:00 a.m. Monday Eastern time), and (ii) any unavailability caused by circumstances beyond Our reasonable control, including, for example, an act of God, act of government, flood, fire, earthquake, civil unrest, act of terror, strike or other labor problem (other than one involving Our employees), Internet service provider failure or delay, third party software, or denial of service attack.

2.2. Protection of Your Data. We will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Your Data, as described in the Documentation, but in any event not less than safeguards as are customary in the electronic health record privacy industry. Those safeguards will include, but will not be limited to, measures for preventing access, use, modification or disclosure of Your Data by Our personnel except (a) to provide the Purchased Services and prevent or address service or technical problems, (b) as compelled by law in accordance with Section 6.3 (Compelled Disclosure) below, or (c) as You expressly permit in writing.

2.3 Our Personnel. We will be responsible for the performance of Our personnel (including Our employees and contractors) and their compliance with Our obligations under this Agreement.

3. USE OF SERVICES

3.1 Licenses. Unless otherwise provided in the applicable Order Form, Services are licensed, and not sold, by Us to You under a non-exclusive, perpetual, non-transferable and worldwide license. All references contained herein or in the Order Forms to the "purchase" or "subscription" of the Purchased Services shall mean the purchase of a license to use the Purchased Services.

3.2 Usage Limits; Right to Audit for Misuse. Services are subject to usage limits as specified in this Agreement and the Order Forms. For each year of the Agreement, You agree to maintain, until two (2) years after such year, complete records and systems relevant to computation and accounting for any payments payable hereunder (including, without limitation, such records and systems which are necessary to confirm that Your use of the Services has not exceeded the number of data points, the types of Permitted Users or other limitations incorporated into the scope of the license granted hereunder such that the fees which You paid hereunder are less than the fees which We would normally receive if the scope of the license were expanded to include Your excess utilization). Separate from the possible Adjustments to License and Software Maintenance Fees prescribed in the applicable Order Form, which are based on future changes in "Base Statistics" (as that term is defined in the applicable Order Form) and upon no less than thirty (30) business days' written notice, We shall have the right, at Our sole discretion, cost and expense, to conduct, through Our employees and independent agents, during Your normal business hours and not more frequently than annually, an audit and review of Your appropriate records and systems to verify amounts paid or payable to Us or Our reseller. The parties shall mutually agree in advance on the scope, method, timing and location of such an audit/review. If the amounts due as determined by the audit are greater than the amounts paid by You, You will be invoiced for the difference. Any deficiency, along with interest at the rate of 0.75% per month, shall be payable within thirty (30) days of such invoice. If the deficiency is greater than five percent (5%) of the amount paid during the period under audit, You shall pay the reasonable expenses associated with such audit, in addition to the deficiency plus interest at the rate of 0.75% per month.

3.3 Your Responsibilities. You will (a) be responsible for Users' compliance with this Agreement and all Order Forms, (b) be responsible for the accuracy, quality and legality of Your Data and the means by which You acquired Your Data, (c) use commercially reasonable efforts to prevent unauthorized access to or use of Services, and notify Us promptly of any such unauthorized access or use, (d) use Services only in accordance with the Documentation and applicable laws and government regulations, and (e) comply with terms of service of non-FairWarning applications with which You use Services.

3.4 Usage Restrictions. You will not (a) make any Service available to, or use any Service for the benefit of, anyone other than You or Permitted Users, (b) sell, resell, license, sublicense, distribute, rent or lease any Service, or include any Service in a service bureau, time sharing or outsourcing offering (provided, however, that if You and We enter into an Order Form which grants reseller rights to You, then You shall have those rights set forth in the Order Form), (c) use a Service to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy rights, (d) use a Service to store or transmit Malicious Code, (e) interfere with or disrupt the integrity or performance of any Service or third-party data contained therein, (f) attempt to gain unauthorized access to any Service or its related systems or networks, (g) permit direct or indirect access to or use of any Service in a way that circumvents a contractual usage limit, (h) copy a Service or any part, feature, function or user interface thereof, (i) frame or mirror any part of any Service, other than framing on Your own intranets or otherwise for Your own internal business purposes or as permitted in the Documentation, (j) access any Service in order to build a competitive product or service, (k) manufacture, sublicense, distribute, transfer, translate, port, upload, post, publish or otherwise dispose of any copies of software or Documentation included in the Services, or (l) reverse assemble, reverse compile or reverse engineer any Service (to the extent such restriction is permitted by law), in whole or in part, nor use any mechanical, electronic or other methods to trace, decompile, disassemble or identify the source code (inclusive of literal content, structure, organization, concepts, technology and methods) of the Services, in whole or in part.

4. FEES AND PAYMENT FOR PURCHASED SERVICES

4.1. Fees. You will pay all fees specified in Order Forms. Except as otherwise specified herein or in an Order Form, (i) fees are based on Services purchased and not actual usage, (ii) payment obligations are non-cancelable and fees paid are non-refundable, and (iii) quantities purchased cannot be decreased during the relevant term.

4.2. Invoicing and Payment. You will provide Us with valid and updated Automated Clearing House (ACH) information, or with a valid purchase order or alternative document reasonably acceptable to Us. If You provide ACH information to Us, You authorize Us to charge your ACH account for all Purchased Services listed in the Order Form for the initial term and any renewal term(s) as set forth in Section 10.2 (Term of Purchased Services). Such charges shall be made in advance, either annually or in accordance with any different billing frequency stated in the applicable Order Form. If the Order Form specifies that payment will be by a method other than ACH, We will invoice You in advance and otherwise in accordance with the relevant Order Form. Invoiced charges are due net 30 days from the invoice date, unless otherwise stated in the Order Form. You are responsible for providing complete and accurate billing and contact information to Us and notifying Us of any changes to such information.

4.3. Overdue Charges. If any invoiced amount is not received by Us by the due date, then without limiting Our rights or remedies, (a) those charges may accrue late interest at the rate of 0.5% of the outstanding balance per month, or the maximum rate permitted by law, whichever is lower, and/or (b) We may condition future subscription renewals and Order Forms on payment terms shorter than those specified in Section 4.2 (Invoicing and Payment).

4.4. Suspension of Service and Acceleration. Subject to Section 4.5 (Payment Disputes), if any amount owing by You under this or any other agreement for Our services is 30 or more days overdue (or 10 or more days overdue in the case of amounts You have authorized Us to charge to Your ACH account) and You have not reasonably disputed the unpaid applicable charges in good faith and are not cooperating diligently to resolve the dispute, We may, without limiting Our other rights and remedies, accelerate Your unpaid fee obligations under such agreements so that all such obligations become immediately due and payable, and suspend Our Services to You until such amounts are paid in full. We will give You at least 10 days' prior notice that Your account is overdue, in accordance with Section 11.2 (Manner of Giving Notice), before suspending Services to You, and We will similarly give you separate written notice and a 60-day opportunity to cure before accelerating Your unpaid fee obligations.

4.5. Payment Disputes. We will not exercise Our rights under Section 4.3 (Overdue Charges) or 4.4 (Suspension of Service and Acceleration) above if You are disputing the applicable charges reasonably and in good faith and are cooperating diligently to resolve the dispute.

4.6. Taxes. Our fees do not include any taxes, levies, duties or similar governmental assessments of any nature, including, for example, value-added, sales, use or withholding taxes, assessable by any jurisdiction whatsoever (collectively, "**Taxes**"). You are responsible for paying all Taxes associated with Your purchases hereunder. If We have the legal obligation to pay or collect Taxes for which You are responsible under this Section 4.6, We will invoice You and You will pay that amount unless You provide Us with a valid tax exemption certificate authorized by the appropriate taxing authority. For clarity, We are solely responsible for taxes assessable against Us based on Our income, property and employees.

4.7. Future Functionality. You agree that Your purchases are not contingent on the delivery of any future functionality or features, or dependent on any oral or written public comments made by Us regarding future functionality or features.

5. PROPRIETARY RIGHTS AND LICENSES

5.1. Reservation of Rights. Subject to the limited rights expressly granted hereunder, We and Our licensors reserve all of Our/their right, title and interest in and to the Services, including all of Our/their related intellectual property rights. No rights are granted to You hereunder other than as expressly set forth herein. Title to and ownership of all complete and partial copies of the Services (including any and all customizations and/or enhancements), whether provided by Us or made by You, whether in machine readable, printed, or other form and including without limitation all revisions, enhancements, technical knowhow, patent rights, copyrights, trademarks, trade secrets and all other proprietary rights pertaining to the Services, are and will remain the sole property of Us. Any copy, modification, revision, enhancement, adaptation, translation, or derivative work of or created from the Services shall be owned solely and exclusively by Us.

5.2. License by You to Host Your Data. You grant Us and Our Affiliates a, limited-term license to host (if applicable), copy, transmit and display Your Data, as necessary for Us to provide the Services

in accordance with this Agreement. Subject to the limited licenses granted herein, We acquire no right, title or interest from You or Your licensors under this Agreement in or to Your Data.

5.3. License by You to Use Feedback. You grant to Us and Our Affiliates a worldwide, perpetual, irrevocable, royalty-free license to use and incorporate into the Services any suggestion, enhancement request, recommendation, correction or other feedback provided by You or Users relating to the operation of the Services.

5.4. Federal Government End Use Provisions. We provide the Services, including related software and technology, for ultimate federal government end use solely in accordance with the following: Government technical data and software rights related to the Services include only those rights customarily provided to the public as defined in this Agreement. This customary commercial license is provided in accordance with FAR 12.211 (Technical Data) and FAR 12.212 (Software) and, for Department of Defense transactions, DFAR 252.227-7015 (Technical Data – Commercial Items) and DFAR 227.7202-3 (Rights in Commercial Computer Software or Computer Software Documentation). If a government agency has a need for rights not granted under these terms, it must negotiate with Us to determine if there are acceptable terms for granting those rights, and a mutually acceptable written addendum specifically granting those rights must be included in any applicable agreement.

5.5. Copyrights. The Services contain material that is protected by United States copyright law and trade secret law, and by international treaty provisions. You shall not remove or alter or permit a third party to remove or alter any proprietary notice of Us from any copy of the Services. Except as provided herein, neither You nor We will use the company name, trademarks, or trade names of the other party without their prior written consent.

6. CONFIDENTIALITY

6.1. Definition of Confidential Information. "**Confidential Information**" generally means all information disclosed by a party ("**Disclosing Party**") to the other party ("**Receiving Party**"), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure. Confidential Information specifically includes, but is not limited to, the following:

(a) Your Confidential Information includes Your Data;

(b) Our Confidential Information includes the Services and Documentation; and

(c) Confidential Information of each party includes the terms and conditions of this Agreement and all Order Forms (including pricing), as well as business and marketing plans, technology and technical information, product plans and designs, and business processes disclosed by such party.

However, Confidential Information does not include any information that (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party, (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party, (iii) is received from a third party without breach of any obligation owed to the Disclosing Party, or (iv) was independently developed by the Receiving Party without use of or reference to Confidential Information of the Disclosing Party.

6.2. Protection of Confidential Information. The Receiving Party (i) will use the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind (but not less than reasonable care), (ii) will not use any Confidential Information of the Disclosing Party for any purpose outside the scope of this Agreement, and (iii) except as otherwise authorized by the Disclosing Party in writing, will limit access to Confidential Information of the Disclosing Party to those of its and its Affiliates' employees and contractors who need that access for purposes consistent with this Agreement and who have signed confidentiality agreements with the Receiving Party containing protections no less stringent than those herein; provided, however, that You shall prevent access to Our Confidential Information by any of such otherwise permitted persons who are engaged in a business or activity which involves the design, development, marketing and/or distribution of products and/or services which are or could be competitive with the Services. Neither party will disclose the terms of this Agreement or any Order Form to any third party other than its Affiliates, legal counsel and accountants without the other party's prior written consent, provided that a party that makes any such

disclosure to its Affiliates, legal counsel or accountants will remain responsible for each such Affiliate's, legal counsel's or accountant's compliance with this Section 6.2.

6.3. Compelled Disclosure. The Receiving Party may disclose Confidential Information of the Disclosing Party to the extent compelled by law to do so, provided the Receiving Party gives the Disclosing Party prior notice of the compelled disclosure (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure. If the Receiving Party is compelled by law to disclose the Disclosing Party's Confidential Information as part of a civil proceeding to which the Disclosing Party is a party, and the Disclosing Party is not contesting the disclosure, the Disclosing Party will reimburse the Receiving Party for its reasonable cost of compiling and providing secure access to that Confidential Information.

6.4. Marketing References. We shall be permitted to verbally identify You as a purchaser of Our Services provided that no Confidential Information is disclosed and such identification will not reasonably be interpreted to constitute an endorsement of Us or Our Services. Under no circumstances will We, without Your prior written approval, (a) issue any written press releases, case studies, or similar materials, or (b) utilize Your name and/or logos on any client list, website, or similar marketing resource made publicly available.

Nothing in this Section 6 is intended to supersede in any way the terms and conditions of the Business Associate Agreement ("BAA") in effect between Us and You. Confidential Information fitting the definition of Protected Information subject to the provisions of the BAA shall be governed by the terms of the BAA and in the event of a conflict, the terms of the BAA shall govern.

7. REPRESENTATIONS, WARRANTIES, EXCLUSIVE REMEDIES AND DISCLAIMERS

7.1. Representations. Each party represents that it has validly entered into this Agreement and has the legal power to do so.

7.2. Our Warranties. We warrant that (a) the Purchased Services will perform materially in accordance with the applicable Documentation, together with any additional Specifications as expressly set forth on the Order Form, (b) We will not materially decrease the functionality of the Purchased Services during a license or subscription term, and (c) the Purchased Services will not introduce Malicious Code into Your systems. For any breach of an above warranty, Your exclusive remedies are those described in Sections 10.3 (Termination) and 10.4 (Refund or Payment upon Termination). Our warranties shall not be effective and We shall have no obligation or liability to You if (i) the Services are not substantially used in accordance with the Documentation; (ii) the Services have been altered, modified or revised by You or any other entity engaged by You without Our written approval; or (iii) the Services are inoperable for any other cause within Your control. We do not warrant or support third party software or services, whether or not they are delivered or designated by Us as "certified" or otherwise, except as expressly specified in a warranty stated in an Order Form.

7.3. Disclaimers. EXCEPT AS EXPRESSLY PROVIDED HEREIN, NEITHER PARTY MAKES ANY WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND EACH PARTY SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. BETA SERVICES ARE PROVIDED "AS IS," EXCLUSIVE OF ANY WARRANTY WHATSOEVER. EACH PARTY DISCLAIMS ALL LIABILITY AND INDEMNIFICATION OBLIGATIONS FOR ANY HARM OR DAMAGES CAUSED BY ANY THIRD-PARTY HOSTING PROVIDERS. WE DO NOT WARRANT THAT THE SERVICES WILL BE PROVIDED UNINTERRUPTED OR ERROR-FREE.

7.4 Insurance. Throughout the term of this Agreement (and, with respect to any policies that are written on a "claims made" basis, for the first three (3) years after any termination of this Agreement), We shall obtain and thereafter maintain, at Our sole cost and expense: (i) a commercial general liability insurance policy in an annual coverage amount of not less than one million dollars ($1,000,000) per occurrence or claim and two million dollars ($2,000,000) in the aggregate, for claims made related to Our performance under this Agreement and all Order Forms; (ii) professional liability (errors and omissions) insurance coverage with an annual limit of not less than two million dollars ($2,000,000); and (iii) "cyber liability" insurance (including, but not necessarily limited to, coverage regarding technology products (hardware, firmware, and software), technology information and services, media liability, Internet media content, network security liability, Web content liability, Internet professional

liability, physical theft of data, and identity theft) having an annual aggregate coverage limit of not less than two million dollars ($2,000,000), to protect against any claims and damages suffered as a result of, or in connection with, any electronic data processing errors and omissions arising out of Our performance under this Agreement (including, but not limited to, any security incident or breach with respect to any Confidential Information) or any breach by Us under any Order Forms or Business Associate Agreement signed by You and Us. Upon Your request from time to time, We will provide current certificates of insurance to You confirming the existence of the insurance coverage described above. Nothing in this Section 7.4 is intended to limit Our liability hereunder to the insurance coverage described.

8. MUTUAL INDEMNIFICATION

8.1. Indemnification by Us. We will defend You against any claim, demand, suit or proceeding made or brought against You by a third party alleging that the use of a Purchased Service in accordance with this Agreement infringes or misappropriates such third party's intellectual property rights or violates applicable law (a "**Claim Against You**"), and will indemnify You from any damages, attorney fees and costs You incur as a result of, or for amounts paid by You under a court-approved settlement or a settlement We approve of, a Claim Against You, provided You (a) promptly give Us written notice of the Claim Against You, (b) give Us sole control of the defense and settlement of the Claim Against You (except that We may not settle any Claim Against You unless it unconditionally releases You of all liability), and (c) give Us all reasonable assistance, at Our expense. If We receive information about an infringement or misappropriation claim related to a Service, We may in Our discretion and at no cost to You (i) modify the Service so that it no longer infringes or misappropriates, without breaching Our warranties under Section 7.2 (Our Warranties), (ii) obtain a license for Your continued use of that Service in accordance with this Agreement, or (iii) terminate Your subscriptions for that Service upon 30 days' written notice and refund You any prepaid fees covering the remainder of the term of the terminated subscriptions. The above defense and indemnification obligations do not apply to the extent a Claim Against You arises from either third party software not provided to You by Us (including on a contributory basis) or Your breach of this Agreement causing such Claim Against You.

8.2. Indemnification by You. You will defend Us against any claim, demand, suit or proceeding made or brought against Us by a third party alleging that Your Data, or Your use of any Service in breach of this Agreement or any Order Form, infringes or misappropriates such third party's intellectual property rights or violates applicable law (a "**Claim Against Us**"), and will indemnify Us from any damages, attorney fees and costs incurred by Us as a result of, or for any amounts paid by Us under a court-approved settlement or a settlement You approve of, a Claim Against Us, provided We (a) promptly give You written notice of the Claim Against Us, (b) give You sole control of the defense and settlement of the Claim Against Us (except that You may not settle any Claim Against Us unless it unconditionally releases Us of all liability), and (c) give You all reasonable assistance, at Your expense.

8.3. Exclusive Remedy. This Section 8 states the indemnifying party's sole liability to, and the indemnified party's exclusive remedy against, the other party for any type of claim described in this Section 8.

9. LIMITATION OF LIABILITY

9.1 Limitation of Liability. NEITHER PARTY'S LIABILITY WITH RESPECT TO ANY SINGLE INCIDENT ARISING OUT OF OR RELATED TO THIS AGREEMENT OR ANY DOCUMENTS EXECUTED IN CONNECTION HEREWITH WILL EXCEED THE AMOUNT PAID BY YOU HEREUNDER IN THE 12 MONTHS PRECEDING THE INCIDENT, PROVIDED THAT IN NO EVENT WILL EITHER PARTY'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT AND ALL DOCUMENTS EXECUTED IN CONNECTION HEREWITH EXCEED THE TOTAL AMOUNT PAID BY YOU HEREUNDER. THE ABOVE LIMITATIONS WILL APPLY WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY. HOWEVER, THE ABOVE LIMITATIONS WILL NOT APPLY TO CLAIMS ARISING FROM BREACHES OF SECTIONS 3.3 (YOUR RESPONSIBILITIES), 3.4 (USAGE RESTRICTIONS), 5 (PROPRIETARY RIGHTS AND LICENSES), 6 (CONFIDENTIALITY), OR 8 (MUTUAL INDEMNIFICATION), NOR LIMIT YOUR PAYMENT OBLIGATIONS UNDER SECTION 4 (FEES AND PAYMENT FOR PURCHASED SERVICES). NOR WILL SUCH LIMITATIONS APPLY TO CLAIMS ARISING FROM A VIOLATION OF ANY HIPAA OR A STATE DATA PRIVACY LAWS, OR THE BREACH OF ANY BUSINESS ASSOCIATE AGREEMENT SIGNED BY AND BETWEEN THE PARTIES RELATING TO THE PRIVACY, SECURITY, OR SAFEGUARDING OF PHI OR OTHER SIMILARLY-PROTECTED INFORMATION.

9.2. Exclusion of Consequential and Related Damages. IN NO EVENT WILL EITHER PARTY HAVE ANY LIABILITY TO THE OTHER PARTY FOR ANY BUSINESS INTERRUPTION, LOSS OF DATA, LOST PROFITS, LOST REVENUES OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, COVER OR PUNITIVE DAMAGES, WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY, EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING DISCLAIMER WILL NOT APPLY TO THE EXTENT PROHIBITED BY LAW OR WITH RESPECT TO CLAIMS ARISING UNDER SECTIONS 3.4 (USAGE RESTRICTIONS), 5 (PROPRIETARY RIGHTS AND LICENSES), 6 (CONFIDENTIALITY), OR 8 (MUTUAL INDEMNIFICATION). NOR WILL SUCH DISCLAIMER APPLY TO CLAIMS ARISING FROM A VIOLATION OF ANY HIPAA OR A STATE DATA PRIVACY LAWS, OR THE BREACH OF ANY BUSINESS ASSOCIATE AGREEMENT SIGNED BY AND BETWEEN THE PARTIES RELATING TO THE PRIVACY, SECURITY, OR SAFEGUARDING OF PHI OR OTHER SIMILARLY-PROTECTED INFORMATION.

10. TERM AND TERMINATION

10.1 Term of Agreement. This Agreement commences on the Effective Date (as defined on page one above) and continues until the terms of all licenses and subscriptions under Order Forms issued hereunder have expired or have been terminated.

10.2. Term of Purchased Services. The term of each license or subscription shall be as specified in the applicable Order Form.

10.3. Termination. A party may terminate this Agreement for cause (i) upon 30 days' written notice to the other party of a material breach if such breach remains uncured at the expiration of such period, or (ii) if the other party becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors, and if involuntarily filed against such party such petition or other proceeding is not withdrawn or discharged within sixty (60) days after notice thereof from the other party. The term of each Order Form shall be as specified therein.

10.4. Refund or Payment upon Termination. If this Agreement is terminated by You in accordance with Section 10.3 (Termination), We will refund You any prepaid fees covering the remainder of the term of all Order Forms after the effective date of termination. If this Agreement is terminated by Us in accordance with Section 10.3, You will pay to Us any unpaid fees covering the remainder of the term of all Order Forms. In no event will termination relieve You of Your obligation to pay any fees payable to Us for the period prior to the effective date of termination.

10.5. Your Data Portability and Deletion. Upon request by You made within 30 days after the effective date of termination or expiration of this Agreement, We will make Your Data available to You for export or download as provided in the Documentation. After that 30-day period, We will have no obligation to maintain or provide Your Data, and will thereafter delete or destroy all copies of Your Data in Our systems or otherwise in Our possession or control as provided in the Documentation, unless legally prohibited.

10.6. Surviving Provisions. The Sections titled "Your Responsibilities," "Usage Restrictions," "Fees and Payment for Purchased Services," "Proprietary Rights and Licenses," "Confidentiality," "Disclaimers," "Mutual Indemnification," "Limitation of Liability," "Exclusion of Consequential and Related Damages," "Refund or Payment upon Termination," "Your Data Portability and Deletion," "Who You Are Contracting With, Notices, Governing Law and Jurisdiction," and "General Provisions" will survive any termination or expiration of this Agreement.

11. WHO YOU ARE CONTRACTING WITH, NOTICES, GOVERNING LAW AND JURISDICTION

11.1. General. Who You are contracting with under this Agreement or any Order Form, who You should direct notices to under this Agreement or any Order Form, what law will apply in any lawsuit arising out of or in connection with this Agreement or any Order Form, and which courts have jurisdiction over any such lawsuit, depend on where You are domiciled.

If You are domiciled (as referenced in the Order Form) in:	You are contracting with:	Notices should be addressed to:	The governing law is:	The courts having exclusive jurisdiction are:
The United States of America	FairWarning, Inc., a Florida corporation, or FairWarning Services, LLC, a Florida limited liability company, as designated on the Order Form	13535 Feather Sound Dr. Clearwater, FL 33762 Attn: Kurt J. Long, President and CEO Email: kurt@fairwarningaudit.com	The laws of the State in which your principal office is located (as referenced on the Order Form) and controlling United States federal law	The state and federal courts in and for the county or province in which Your principal office is located (as referenced on the Order Form)
A Country in Europe	FairWarning Software Limited, a United Kingdom company	13535 Feather Sound Dr. Clearwater, FL 33762 Attn: Kurt J. Long, President and CEO Email: kurt@fairwarningaudit.com	England	England
		In all cases, with a copy (which shall not constitute notice) to: Randolph J. Wolfe, Esq. Foley & Lardner LLP 100 N. Tampa Street Suite 2700 Tampa, FL 33602 Email: rwolfe@foley.com		

11.2. Manner of Giving Notice. Except as otherwise specified in this Agreement, all notices, permissions and approvals hereunder shall be (a) in writing, (b) given via: (i) personal delivery, (ii) certified mail, return receipt requested, (iii) Federal Express, DHL or other reputable expedited courier service, or (iv) email (provided email shall not be sufficient for notices of termination or an indemnifiable claim), and (c) deemed given only upon actual receipt or rejection of delivery (provided, however, that notices, permissions and approvals given via email outside of the normal business hours of the addressee shall not be deemed given until the commencement of the addressee's next business day). Billing-related notices to You shall be addressed to the relevant billing contact

designated by You. All other notices to You shall be addressed to the relevant Services system administrator designated by You.

11.3. Agreement to Governing Law and Jurisdiction. Each party agrees to the applicable governing law above without regard to choice or conflicts of law rules, and to the exclusive jurisdiction of the applicable courts above.

11.4 Waiver of Jury Trial. FOR ALL EQUITABLE PROCEEDINGS, THE PARTIES HEREBY EXPRESSLY WAIVE ANY AND ALL RIGHT TO A TRIAL BY JURY WITH RESPECT TO ANY EQUITABLE RELIEF BEING SOUGHT. THE PRECEDING SENTENCE SHALL NOT LIMIT THE PARTIES' RIGHTS TO SUBSEQUENTLY BRING SEPARATE ACTIONS OR PROCEEDINGS SEEKING DAMAGES OR OTHER NON-EQUITABLE RELIEF.

12. GENERAL PROVISIONS

12.1. Export Compliance. The Services We make available and derivatives thereof may be subject to export laws and regulations of the United States and other jurisdictions. Each party represents that it is not named on any U.S. government denied-party list. You shall not permit Users to access or use any Service in a U.S.-embargoed country (currently Cuba, Iran, North Korea, Sudan or Syria) or in violation of any U.S. export law or regulation.

12.2. Anti-Corruption. You have not received or been offered any illegal or improper bribe, kickback, payment, gift, or thing of value from any of Our employees or agents in connection with this Agreement. Reasonable gifts and entertainment provided in the ordinary course of business do not violate the above restriction. If You learn of any violation of the above restriction, You will use reasonable efforts to promptly notify Our Legal Department at legal@fairwarning.com.

12.3 Entire Agreement and Order of Precedence. This Agreement is the entire agreement between You and Us regarding Your use of Services and supersedes all prior and contemporaneous agreements, proposals or representations, written or oral, concerning its subject matter; provided, however, that this Agreement does not supersede any Business Associate Agreement signed by and between the parties relating to the parties' obligations under HIPAA. No modification, amendment, or waiver of any provision of this Agreement will be effective unless in writing and signed by both parties. The parties agree that any term or condition stated in Your purchase order or in any other of Your order documentation (excluding Order Forms) is void. In the event of any conflict or inconsistency among the following documents, the order of precedence shall be: (1) any Business Associate Agreement signed by and between the parties relating to the parties' obligations under HIPAA, (2) the applicable Order Form, (3) this Agreement, and (4) the Documentation.

12.4. Assignment. Neither party may assign any of its rights or obligations hereunder, whether by operation of law or otherwise, without the other party's prior written consent (not to be unreasonably withheld); provided, however, either party may assign this Agreement in its entirety (including all Order Forms), without the other party's consent to its Affiliate or in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets. Notwithstanding the foregoing, if a party is acquired by, sells substantially all of its assets to, or undergoes a change of control in favor of, a direct competitor of the other party, then such other party may terminate this Agreement (including all Order Forms) upon written notice. In the event of such a termination, We will refund to You any prepaid maintenance and support fees covering the remainder of the term of all subscriptions. Subject to the foregoing, this Agreement will bind and inure to the benefit of the parties, their respective successors and permitted assigns.

12.5. Relationship of the Parties. The parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties.

12.6. Third-Party Beneficiaries. Other than the third party Affiliates (which, if applicable, shall be expressly identified in the applicable Order Form and are defined as "Non-Affiliates" in the Order Forms entered into concurrently with this Agreement), there are no third-party beneficiaries under this Agreement.

12.7. Waiver. No failure or delay by either party in exercising any right under this Agreement will constitute a waiver of that right.

12.8. Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, the provision will be deemed null and void, and the remaining provisions of this Agreement will remain in effect.

12.9 Force Majeure. Neither party shall be responsible for failures of its obligations under this Agreement or any Order Forms to the extent that such failure is due to causes beyond such party's control, including, but not limited to, acts of God, war, terrorism or threat thereof, acts of any government or agency thereof, fire, explosions, epidemics, quarantine restrictions, strikes, lockouts, embargoes, severe weather conditions, delay in transportation, or delay of suppliers or subcontractors; provided, however, that Your obligation to timely make payment of all fees for Purchased Services may be temporarily delayed during the event, but shall not be excused or further delayed by this clause.

Attachment I

HIPAA Business Associate Agreement
Addendum to Contract

Between the County of Riverside and FairWarning Services, LLC

This HIPAA Business Associate Agreement (the "Addendum") supplements, and is made part of the Underlying Agreement between the County of Riverside ("County") and FairWarning Services, LLC ("Contractor") and shall be effective as of the date the Underlying Agreement approved by both Parties (the "Effective Date").

RECITALS

WHEREAS, County and Contractor entered into the Underlying Agreement pursuant to which the Contractor 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 Contractor for the purposes of carrying out its obligations under the Underlying Agreement;

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;

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

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

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;

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;

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 Contractor 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 Contractor during the course of performing functions, services and activities on behalf of County, and appropriate limitations and conditions on such uses and disclosures;

WHEREAS, County has contracted with Contractor in the Underlying Agreement to utilize Contractor's software solution and professional services to find and investigate County's own potential Breaches of PHI and/or ePHI that occur within County's own information technology and electronic health record systems; and

WHEREAS, neither Contractor nor County intends for this Addendum to impose the reporting or mitigation obligations regarding Breaches of Unsecured PHI and Security Incidents that occur (a) within County's information systems or at County's facilities, and (b) through no contributory role or fault of Contractor; and

WHEREAS, the terms of this Addendum shall not be construed in any way to limit County's rights and Contractor's obligations under the Underlying Agreement.

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 Contractor 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.

         (d) Any unauthorized acquisition, access, disclosure, or use of PHI and ePHI in which neither Contractor nor its subcontractors or agents has had any contributory role or fault.

   B. "Business associate" has the meaning given such term in 45 CFR §160.103, 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. Security Incident shall, however, exclude any attempted or successful Security Incident that does not occur within Contractor's information systems and in which neither Contractor nor its subcontractors or agents has had any contributory role or fault.

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 Contractor of County's PHI and/or ePHI.**

A. Except as otherwise provided in this Addendum, Contractor may use, disclose, or access PHI and/or ePHI as necessary to perform any and all obligations of Contractor 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), Contractor may:

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

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

a) The disclosure is required by law; or,

b) Contractor obtains reasonable assurances, in writing, from the person to whom Contractor 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 Contractor 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 Contractor 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. Contractor 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. Contractor 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. Contractor agrees not to make any disclosure of PHI and/or ePHI that County would be prohibited from making.

D. Contractor 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. Contractor 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 Contractor for services provided pursuant to the Underlying Agreement.

4. **Obligations of County.**

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

B. County agrees to make its best efforts to promptly notify Contractor 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 Contractor's ability to perform its obligations under the Underlying Agreement, or this Addendum.

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

D. County agrees not to request Contractor 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 Contractor can perform its obligations under this Addendum and/or Underlying Agreement.

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

A. Use or disclose PHI only if such use or disclosure complies with each applicable requirement of 45 CFR §164.504(e). Contractor 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. Contractor shall promptly notify County if Contractor 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 and to the extent Contractor is responsible for, any harmful effect that is known to Contractor of a use or disclosure of PHI and/or ePHI by or through Contractor, its subcontractors or agents in violation of this Addendum.

E. Report to County any use or disclosure of PHI and/or ePHI by or through Contractor, its subcontractors or agents, not provided for by this Addendum or otherwise in violation of HITECH, HIPAA, the Privacy Rule, and/or Security Rule of which Contractor 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 subcontractors that create, receive, maintain, transmit or access PHI on behalf of the Contractor agree through contract to equally stringent restrictions and conditions that apply to Contractor with respect to such PHI and/or ePHI, including the restrictions and conditions pursuant to this Addendum.

G. Make available to the Secretary, in the time and manner designated by Secretary, Contractor's internal practices, books and records relating to the use, disclosure and privacy protection of PHI received from

County, or created or received by Contractor on behalf of County, for purposes of determining 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(e)(1) 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 Contractor shall promptly notify County upon Contractor'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 by Contractor.

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 Contractor 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 subcontractor of which Contractor becomes aware that constitute a material breach or violation of the subcontractor's obligations under the business associate contract with Contractor, and if such steps are unsuccessful, Contractor agrees to terminate its contract with the subcontractor if feasible.

6. **Access to PHI, Amendment and Disclosure Accounting.** Contractor 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 Contractor uses or maintains electronic health records. Contractor 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 Contractor or Contractor 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, Contractor shall:

A. 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 Contractor creates, receives, maintains, or transmits on behalf of County in accordance with 45 CFR §164.308, §164.310, and §164.312;

B. 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;

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

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

E. Ensure compliance with the Security Rule by Contractor's workforce;

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

G. Report to County any successful security incident of which Contractor becomes aware, including breaches of unsecured PHI as required by 45 CFR §164.410. The parties acknowledge and agree, however, that this Section constitutes notice of the ongoing existence and occurrence of attempted but unsuccessful Security Incidents for which no further notice shall be required. Such unsuccessful Security Incidents shall include, but not be limited to, pings and other broadcast attacks on Contractor 's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in the unauthorized access, Use or Disclosure of County's ePHI; and,

H. 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, Contractor 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, Contractor 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 Contractor as of the first day on which such breach is known to Contractor or, by exercising reasonable diligence, would have been known to Contractor, which includes any person, other than the person committing the breach, who is an employee, officer, or other agent of Contractor (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 Contractor:

a) The identification of each individual whose unsecured PHI has been, or is reasonably believed by Contractor 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 Contractor 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 Contractor, Contractor 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, Contractor 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 Contractor 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, Contractor 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 Contractor'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, Contractor 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 Contractor'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 Contractor's use or disclosure of PHI and/or ePHI violates the Privacy Rule, Contractor shall maintain documentation sufficient to demonstrate that all notifications were made by Contractor as required by 45 CFR Part 164, Subpart D, or that such use or disclosure did not constitute a breach, including Contractor'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) Contractor 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) Contractor 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 Contractor detects such incident. Contractor 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. Contractor 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 claim, demand, suit, or proceeding brought against such entity or person by a third party, based or asserted upon any improper act or omission by Contractor, its officers, employees, subcontractors, agents, or representatives, and arising out of Contractor's performance of services pursuant to the Underlying Agreement, including but not limited to claims of property damage, bodily injury, or death. Contractor shall indemnify and hold harmless County, at Contractor's expense, from all damages, costs, fees, and expenses, including but not limited to reasonable attorney fees, cost of investigation, defense and settlements or awards, of County and its respective directors, officers, Board of Supervisors, elected and appointed officials, employees, agents, or representatives in any such claim, demand, or action based upon such alleged acts or omissions.

B. Subject to applicable state law, County agrees to defend Contractor and its respective officers, Board of Directors, employees, agents, and representatives from any claim, demand, suit, or proceeding brought against such entity or person by a third party, based or asserted upon any improper act or omission by County, its directors, officers, employees, subcontractors, agents, or representatives, and arising out of County's receipt of services pursuant to the Underlying Agreement, including but not limited to claims of property damage, bodily injury, or death. County shall indemnify and hold harmless Contractor, at County's expense, from all damages, costs, fees, and expenses, including but not limited to reasonable attorney fees, cost of investigation, defense and settlements or awards, of Contractor and its respective officers, Board of Directors, employees, agents, or representatives in any such claim, demand, or action based upon such alleged improper acts or omissions.

C. With respect to any action or claim subject to indemnification above, the indemnifying party shall, at its sole cost, have the right to use counsel of their choice, subject to the approval of indemnified party, 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 indemnified party; provided, however, that any such adjustment, settlement or compromise in no manner whatsoever limits or circumscribes indemnifying party's indemnification to indemnified party as set forth herein. Indemnifying party's obligation to defend, indemnify and hold harmless shall be subject to indemnified party's having given 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 Contractor's expense, for the defense or settlement thereof. Contractor's obligation hereunder shall be satisfied when Contractor has provided to County the appropriate form of dismissal relieving County from any liability for the action or claim involved.

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

E. 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 either party from indemnifying the other party to the fullest extent allowed by law.

F. 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 Contractor, or created or received by Contractor 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 this Addendum.

11. **Termination.**

A. **Termination for Breach of Contract.** A material 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 upon receipt of notice, 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, Contractor shall destroy all PHI and/or ePHI received from County, or created or received by the Contractor on behalf of County, and, in the event of destruction, Contractor shall certify such destruction, in writing, to County. This provision shall apply to all PHI and/or ePHI which are in the possession of subcontractors or agents of Contractor. Contractor shall retain no copies of PHI and/or ePHI, except as provided below in paragraph (2) of this section.

2) In the event that Contractor determines that returning or destroying the PHI and/or ePHI is not feasible, Contractor shall provide written notification to County of the conditions that make such return or destruction not feasible. Upon determination by Contractor that return or destruction of PHI and/or ePHI is not feasible, Contractor 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 Contractor maintains such PHI and/or ePHI.

12. **General Provisions.**

A. **Retention Period.** Whenever Contractor is required to document or maintain documentation pursuant to the terms of this Addendum, Contractor shall retain such documentation as is specified herein 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 each party to comply with HITECH, the Privacy Rule, Security Rule, and HIPAA generally.

C. **Survival.** The obligations of Contractor 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 (1) are reasonably related to the security and privacy of PHI and to compliance with data privacy laws and (2) 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 Contractor 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 Contractor 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: 26520 Cactus Avenue,
Moreno Valley, CA 92555

County HIPAA Privacy Officer Phone Number: (951) 486-6471

Riverside University HEALTH SYSTEM

Date: 1/23/2019

From: Lakisha Reese

To: Board of Supervisors/Purchasing Agent

Via: Michelle DeSpain, 951-486-4469 Ext # 64469

Subject: Single Source Procurement; Request for Electronic Health Monitoring System

The below information is provided in support of my Department requesting approval for a sole or single source. (*Outside of a duly declared emergency, the time to develop a statement of work or specifications is not in itself justification for sole or single source.*)

1. **Supplier being requested: Fair Warning**

2. **Vendor ID:** _____

3. x **Single Source** ☐ **Sole Source**
   (*Single Source - is a purchase of a commodity or service without obtaining competitive bids although more than one source is available)*

   (Sole Source - is a purchase of a commodity or service that is proprietary or no other vendor is qualified or willing to meet the county specified requirements)

4. **Have you previously requested and received approval for a sole or single source request for this vendor for your department?** *(If yes, please provide the approved sole or single source number).*

   ☐ **Yes** x **No**
   SSJ# _____

5. **Was the request approved for a different project?**

   ☐ **Yes** x **No**

6. **Supply/Service being requested:**
   (If this request is for professional services, attach the service agreement to this sole source request. The Purchasing Agent, or designee, is the signing authority for agreements unless the service is exempted by Ordinance 459, Board delegated authority or by State law. All

26520 Cactus Avenue, Moreno Valley, CA 92555 / 951-486-4355 / RUHealth.org

Riverside University HEALTH SYSTEM

Insurance requirements must be met prior to work commencement. See the Risk Management website for vendor insurance requirements.)

Fair Warning will flag and alert RUHS Compliance staff of potential HIPAA violations occurring in the EPIC patient system within the hospital. This monitoring system ensures patient privacy remains a priority and is continuously protected.

The Riverside University Health System (RUHS) seeks to improve its compliance services by proactively addressing risks posed by unauthorized access to electronic medical records. Stemming from the HIPAA Privacy Rule that limits disclosure of health information to the minimum necessary for treatment, payment or operations, RUHS has a policy of providing its workforce access to patient protected health information based on a need-to-know to perform their job duties at RUHS. To monitor workforce access to the EPIC system, RUHS-Corporate Compliance utilizes the Fair Warning software that performs regular access checks and sends automated alerts when certain criteria are met.

7. **Unique features of the supply/service being requested from this supplier.** *(If this sole source request is due to proprietary software or machinery, or hardware, provide a supporting letter from the manufacturer. If this is a single source request provide an explanation of how this provides the best value for the County by selecting this vendor.)*

As a member of the Loma Linda University Shared Services EHR Platform, RUHS has an obligation to monitor access to the EPIC system. RUHS has ongoing access to Fair Warning's monitoring services as a satellite customer of Loma Linda University Medical Center (LLU). Under the proposed contract, RUHS will remain a Loma Linda University (LLU) affiliate but will gain administrative control over the automated alerts. While LLU will still host and manage the software licenses, RUHS will be able to select and manage its alerts, separate from LLU giving RUHS greater flexibility over its resources and more control over the types of alerts received (applying filters for false positives or expanding the criteria).

8. **Reasons why my department requires these unique features from the vendor and what benefit will accrue to the county:**

Fair Warning will flag and alert RUHS Compliance staff of potential HIPAA violations occurring in the EPIC patient system within the hospital. This monitoring system ensures patient privacy remains a priority and is continuously protected.

The Riverside University Health System (RUHS) seeks to improve its compliance services by proactively addressing risks posed by unauthorized access to electronic medical records. Stemming from the HIPAA Privacy Rule that limits disclosure of health information to the minimum necessary for treatment, payment or operations, RUHS has a policy of providing its workforce access to patient protected health information based on a need-to-know to perform their job duties at RUHS. To monitor workforce access to the EPIC system, RUHS-Corporate Compliance

Riverside University HEALTH SYSTEM

utilizes the Fair Warning software that performs regular access checks and sends automated alerts when certain criteria are met.

9. Period of Performance: From: March 12, 2019 to July 27, 2020
(total number of years)

Is this an annually renewable contract? X No ☐ Yes
Is this a fixed-term agreement: No x Yes
(A fixed- term agreement is set for a specific amount of time; it is not renewed annually. Ensure multi-year fixed-term agreements include a cancellation, non-appropriation of funds, or refund clause. If there is no clause(s) to that effect, then the agreement must be submitted to the Board for approval. No exemptions shall apply.)

10. Identify all costs for this requested purchase. In addition, please include any single or sole source amounts previously approved and related to this project and vendor in the section designated below for current and future fiscal years. You do not need to include previous fiscal year amounts. If approval is for multiple years, ongoing costs must be identified below. If annual increases apply to ongoing costs such as CPI or other contract increases, provide the estimated annual cost for each consecutive year. If the annual increase may exceed the Purchasing Agent's authority, Board approval must be obtained. *(Note: ongoing costs may include but are not limited to subscriptions, licenses, maintenance, support, etc.)*

Description:	FY 19	FY 20	FY21	FY__	FY__	Total
One-time Costs:	$17,733	$70,932	$5,911.00			$94, 576
(Insert description)						
Ongoing Costs:						
(Insert description)						
Previous SSJ Approved Amounts:						
(Insert description)						
Total Costs	$17,733	$70,932	$5,911.00			$94,576

Note: Insert additional rows as needed

11. Price Reasonableness: *(Explain why this price is reasonable or cost effective – were you provided government discounted pricing? Is this rate/fee comparable to industry standards?)*

Riverside University HEALTH SYSTEM

The contract is for a 16 month term with the option to renew. The contract provides up to eight enforceable policies (automated alerts) RUHS is currently allowed two. In the first year, RUHS may enforce up to four core enforced polices. Implementation of the four-core enforced polices will cost $10,800.00 in the first year. The implementation includes working with Fair Warning analysts to select the areas deemed essential to the success of the Patient Privacy Monitoring Program with improvement and updates as desired. Fair Warning will customize the alert trigger criteria to meet the needs of RUHS.
The monitoring of the contract for the first year, covering the four core enforced policies, will complete the total of $17,773 .The second year will allow RUHS to select an addition four enforced polices, bringing the total of monitored policies to eight. The contracted fee to monitor the eight policies is $76,803

Because LLU hosts the software, there are no additional fees and no ongoing operational commitment for the County. The total cost of the contract for sixteen months is $94,576.00

12. Projected Board of Supervisor Date (if applicable): March 12, 2019
(Draft Form 11s, service agreement and or quotes must accompany the sole source request for Purchasing Agent approval.)

Riverside University HEALTH SYSTEM

Jennifer Quikshank

Department Head Signature (or designee) | Print Name | Date

The section below is to be completed by the Purchasing Agent or designee.

Purchasing Department Comments:

Approve | **Approve with Condition/s** | **Disapprove**

Condition/s:

Board approval is required for renewal past 7/27/20.

Not to exceed:

☐ **One-time** $_____

☐ **Annual Amount** $_____ / per fiscal year through _____(date)
(If Annual Amount Varies each FY)

FY 18/19: $ 17,733
FY 19/20: $ 70,932
FY 20/21: $ 5,911
FY _____: $_____

FY _____: $_____

2/19/19 | 19-109

Purchasing Agent | **Date** | **Approval Number** (Reference on Purchasing Documents)