



County of Santa Clara

Office of the County Executive
Procurement Department
150 W. Tasman Dr. First Floor
San Jose, CA 95134
Telephone 408-491-7400 • Fax 408-491-7496

**SEVENTH AMENDMENT TO AGREEMENT NO. 5500002793
BY AND BETWEEN
THE COUNTY OF SANTA CLARA
AND ABBOTT RAPID DIAGNOSTICS INFORMATICS, INC.**

This is the Seventh Amendment to the Agreement No.5500002793 between the County of Santa Clara ("County" or "Customer") and Abbott Rapid Diagnostics Informatics, Inc. ("ARDx Informatics" or "Contractor") entered into on January 10, 2017 to provide Software License and Support for the County.

This Agreement is amended as follows effective on July 10, 2022.

1. **Key Provisions** are amended as follows:

1.1 **AGREEMENT TERM** is revised to read:

"This Agreement commences on January 10, 2017 and expires July 9, 2027, unless terminated earlier or otherwise amended."

1.2 **TOTAL AGREEMENT VALUE** is revised to read:

"The total not to exceed value of this Agreement is \$1,000,000, which represents an increase of \$526,484.50 from the prior not to Exceed amount of \$473,515.5.

ARDx Informatics understands that the not to exceed value does not represent a commitment by County to ARDx Informatics."

2. Add **Exhibit B-6, Price Summary and Compensation Plan**, attached hereto and incorporated herein by this reference.
3. Replace **Exhibit D, Business Associate Agreement** with **Exhibit D-1, Business Associate Agreement**. attached hereto and incorporated herein by this reference.

Board of Supervisors: Mike Wasserman, Cindy Chavez, Otto Lee, Susan Ellenberg, S. Joseph Simitian
County Executive: Jeffrey V. Smith

4. Replace **Exhibit E, Vendor Remote Access and User Responsibility Agreements** with **Exhibit E-1, County Information Technology User Responsibility Statement for Third Parties**, attached hereto and incorporated herein by this reference.
5. Add **Exhibit F, Remote Access**, attached hereto and incorporated herein by this reference.
6. Add **Exhibit G, Contractor Certification Of Compliance With Covid-19 Vaccine Requirements**, attached hereto and incorporated herein by this reference.
7. Add **Exhibit I, Insurance Requirements For Professional Services Contracts**, attached hereto and incorporated herein by this reference.
8. **Exhibit A, County of Santa Clara Terms and Conditions** is amended as follows:

8.1. Section 49 "County Data" is hereby deleted and replaced with the following:

49. COUNTY DATA

- (1) Contractor shall not acquire any ownership interest in County Data (including County Confidential Information). As between ARDx Informatics and County, all pertinent County Confidential Information and/or County Data shall remain the property of the County. ARDx Informatics shall not, without County's written permission, use or disclose County Data (including County Confidential Information) other than in the performance of its obligations under this Agreement.
- (2) Contractor shall be responsible for establishing and maintain an information security program that is designed to ensure the security and confidentiality of County Data, protect against any anticipate threats or hazards to the security or integrity of County Data, and protect against unauthorized access to or use of County Data that could result in substantial harm or inconvenience to County or any end users. Upon termination or expiration of this Agreement, Contractor shall seek and follow County's direction regarding the proper disposition of County Data.
- (3) Contractor shall be responsible for ensuring compliance by its officers, employees, agents, and subcontractors with the confidentiality, privacy, and information security requirements of this Agreement. Should County Confidential Information and/or legally protected County Data be divulged to unauthorized third parties, Contractor shall comply with all applicable federal and state laws and regulations, including but not limited to California Civil Code sections 1798.29 and 1798.82 at Contractor's sole expense. Contractor shall not charge County for any expenses associated with Contractor's compliance with these obligations.
- (4) Contractor shall defend, indemnify and hold County harmless against any claim, liability, loss, injury or damage arising out of, or in connection with, the unauthorized use, access, and/or disclosure of information by Contractor and/or its agents, employees or sub-contractors, excepting only loss, injury or damage caused by the sole negligence or willful misconduct of personnel employed by the County.

8.2. Sections 45 "Nondiscrimination" and 69 "Wage Theft Prevention" are hereby deleted in their entirety and replaced with the following:

45. NON-DISCRIMINATION. Intentionally deleted.

**69. COMPLIANCE WITH ALL LAWS AND REGULATIONS INCLUDING
NONDISCRIMINATION, EQUAL OPPORTUNITY, AND WAGE THEFT PREVENTION**

Contractor's violation of this provision shall be deemed a material default by Contractor, giving County a right to terminate the Agreement. Examples of such Regulations include but are not limited to California Occupational Safety and Health Act of 1973, Labor Code §6300 *et seq.* the Fair Packaging and Labeling Act. and the standards and regulations issued there under. Contractor agrees to indemnify and hold harmless the County for any loss, damage, fine, penalty, or any related expense as a result of Contractor's failure to comply with the act and any standards or regulations issued there under.

- (1) Compliance with All Laws. Contractor shall comply with all applicable Federal, State, and local laws, regulations, rules, and policies (collectively, "Laws"), including but not limited to the non-discrimination, equal opportunity, and wage and hour Laws referenced in the paragraphs below.
- (2) Compliance with Non-Discrimination and Equal Opportunity Laws: Contractor shall comply with all applicable Laws concerning nondiscrimination and equal opportunity in employment and contracting, including but not limited to the following: Santa Clara County's policies for contractors on nondiscrimination and equal opportunity; Title VII of the Civil Rights Act of 1964 as amended; Americans with Disabilities Act of 1990; the Age Discrimination in Employment Act of 1967; the Rehabilitation Act of 1973 (Sections 503 and 504); the Equal Pay Act of 1963; California Fair Employment and Housing Act (Government Code sections 12900 *et seq.*); California Labor Code sections 1101, 1102, and 1197.5; and the Genetic Information Nondiscrimination Act of 2008. In addition to the foregoing, Contractor shall not discriminate against any subcontractor, employee, or applicant for employment because of age, race, color, national origin, ancestry, religion, sex, gender identity, gender expression, sexual orientation, mental disability, physical disability, medical condition, political belief, organizational affiliation, or marital status in the recruitment, selection for training (including but not limited to apprenticeship), hiring, employment, assignment, promotion, layoff, rates of pay or other forms of compensation. Nor shall Contractor discriminate in the provision of services provided under this contract because of age, race, color, national origin, ancestry, religion, sex, gender identity, gender expression, sexual orientation, mental disability, physical disability, medical condition, political beliefs, organizational affiliations, or marital status.
- (3) Compliance with Wage and Hour Laws: Contractor shall comply with all applicable wage and hour Laws, which may include but are not limited to, the Federal Fair Labor Standards Act, the California Labor Code, and, if applicable, any local Minimum Wage, Prevailing Wage, or Living Wage laws.
- (4) Definitions: For purposes of this Section, the following definitions shall apply. A "Final Judgment, Decision, Determination, or Order" shall mean a judgment, decision, determination, or order (a) which is issued by a court of law, an investigatory government agency authorized by law to enforce an applicable Law, an arbiter, or arbitration panel and (b) for which all appeals have been exhausted or the time period to appeal has expired. For pay equity Laws, relevant investigatory government agencies include the federal Equal Employment Opportunity Commission, the California Division of Labor Standards Enforcement, and the California Department of Fair Employment and Housing. Violation of a pay equity Law shall mean unlawful discrimination in compensation on the basis of an individual's sex, gender, gender identity, gender expression, sexual orientation, race, color, ethnicity, or national origin under Title VII of the Civil Rights Act of 1964 as amended, the Equal Pay Act of 1963, California Fair Employment and Housing Act, or California Labor Code section 1197.5, as applicable. For wage and hour Laws, relevant investigatory

government agencies include the federal Department of Labor, the California Division of Labor Standards Enforcement, and the City of San Jose's Office of Equality Assurance.

- (5) Prior Judgments, Decisions or Orders against Contractor: By signing this Agreement, Contractor affirms that it has disclosed any final judgments, decisions, determinations, or orders that (a) were issued in the five years prior to executing this Agreement by a court or investigatory government agency and (b) found that Contractor violated an applicable wage and hour or pay equity law. Contractor further affirms that it has satisfied and complied with – or has reached agreement with the County regarding the manner in which it will satisfy – any such final judgments, decisions, determinations, or orders.
- (6) Violations of Wage and Hour Laws or Pay Equity Laws During Term of Agreement: If at any time during the term of this Agreement, Contractor receives a Final Judgment, Decision, Determination, or Order rendered against it for violation of an applicable wage and hour Law or pay equity Law, then Contractor shall satisfy and comply with any such Final Judgment, Decision, Determination, or Order. Contractor shall inform the Office of the County Executive Office of Countywide Contracting Management (OCCM) of any relevant Final Judgment, Decision, Determination, or Order against it within 30 days of the Final Judgment, Decision, Determination, or Order becoming final or learning of the Final Judgment, Decision, Determination, or Order, whichever is later. Contractor shall also provide any documentary evidence of compliance with the Final Judgment, Decision, Determination, or Order within 15 days of satisfying the Final Judgment, Decision, Determination, or Order. Any notice required by this paragraph shall be addressed to the Office of the County Executive OCCM at 70 West Hedding Street, East Wing, 11th Floor, San Jose, CA 95110. Notice provisions in this paragraph are separate from any other notice provisions in this Agreement and, accordingly, only notice provided to the Office of the County Executive OCCM satisfies the notice requirements in this paragraph.
- (7) Access to Records Concerning Compliance with Pay Equity Laws: In addition to and notwithstanding any other provision of this Agreement concerning access to Contractor's records, Contractor shall permit the County and/or its authorized representatives to audit and review pertinent and responsive records related to compliance with applicable pay equity Laws. Upon the County's request, Contractor shall provide the County with access to any and all such records, including but not limited to financial and employee records, that are related to the purpose of this Section, except where prohibited by federal or state laws, regulations, or rules, or protected by attorney-client privilege. County's access to such records and facilities shall be permitted at any time during Contractor's normal business hours upon no less than 15 business days' advance notice.
- (8) Pay Equity Notification: Contractor shall (1) directly provide each employee working in California and each person applying for a job in California with a written copy of any applicable pay equity Laws, or (2) electronically disseminate the text of applicable pay equity Laws to each California employee and job applicant, either directly or by posting a copy in conspicuous places available to employees and applicants. Such notification shall occur at least once during the term of this Agreement and, if this Agreement is a multi-year Agreement, at least annually thereafter.
- (9) Material Breach: Failure to comply with any part of this Section shall constitute a material breach of this Agreement. In the event of such a breach, the County may, in its discretion, exercise any or all remedies available under this Agreement and/or at law. County may, among other things, take any or all of the following actions:
- (i) suspend or terminate any or all parts of this Agreement;
 - (ii) withhold payment on any disputed invoices to Contractor until full satisfaction of a Final Judgment, Decision, Determination, or Order;
 - (iii) Offer Contractor an opportunity to cure the breach.

(10) Subcontractors: Intentionally deleted.

8.3. Section 71. "Contracting Principles" is added and shall read as follows:

"71. CONTRACTING PRINCIPLES

All entities that contract with the County to provide services where the contract value is \$100,000 or more per budget unit per fiscal year and/or as otherwise directed by the Board, shall be fiscally responsible entities and shall treat their employees fairly. To ensure compliance with these contracting principles, all contractors shall: (1) comply with all applicable federal, state and local rules, regulations and laws; (2) maintain financial records, and make those related records available upon request; (3) upon request, provide to the County copies of any related financial audits that have been completed during the term of the Agreement; (4) upon the County's request, provide the County reasonable access, through representatives of the Contractor, to associated facilities, and financial that are related to the purpose of the Agreement, except where prohibited by federal or state laws, regulations or rules."

8.4 Section 72. "COVID-19 Requirements" is added and shall read as follows:

"72. COVID-19 REQUIREMENTS

Contractor shall comply with all County requirements relating to COVID-19 for persons who routinely perform services for the County onsite and share airspace with or proximity to other people at a County facility as part of their services for the County, including but not limited to vaccination, as applicable and periodically updated, and available at <https://procurement.sccgov.org/doing-business-county/contractor-vaccinations> and incorporated herein by this reference. If applicable, Contractor shall complete the Contractor Certification of Compliance with COVID-19 Vaccine Requirements ("Certification"), attached hereto as Exhibit G. Contractor shall comply with the requirements of this Section for the entire term of this Agreement.

Contractor shall comply with all reasonable requests by County for documentation demonstrating Contractor's compliance with this Section. Failure by Contractor to comply with any of the requirements of this Section (including but not limited to vaccination and masking requirements and completion and submittal of the Certification) is a material breach of this Agreement, and the County may, in its sole discretion terminate this Agreement immediately or take other action as the County may determine to be appropriate."

All other terms and conditions of the Agreement remain in full force and effect. In the event of a conflict between the original Agreement and this Amendment, this Amendment controls.

Prepared and administered by: Alex Qin, Buyer I at (408) 491-7441 or Alex.Qin@prc.sccgov.org

The Agreement No. 5500002793 as amended constitutes the entire agreement of the parties concerning the subject matter herein and supersedes all prior oral and written agreements, representations and understandings concerning such subject matter.

By signing below, signatory warrants and represents that he/she executed this Amendment in his/her authorized capacity, that he/she has the authority to bind the entity listed below to contractual obligations and that by his/her signature on this Amendment, the entity on behalf of which he/she acted, executed this Amendment.

COUNTY OF SANTA CLARA

ABBOTT RAPID DIAGNOSTICS
INFORMATICS, INC

DS
15 DocuSigned by:
Long Zhang
82D7984E4AED476...

DocuSigned by:
Abe Neudorf
By: FCC646B2644E4E8...

For: Director of Procurement

Name: Abe Neudorf

Title: Controller

Date: 6/28/2022

Date: 6/27/2022

DocuSigned by:
Michael Kulpa
By: 975CC95AA962476...

APPROVED AS TO FORM AND LEGALITY

DocuSigned by:
Sara J Ponzio 6/27/2022
4B974B9E689D4D9...

Name: Michael Kulpa

Title: National Sales Director

Date: 6/27/2022

Sara J. Ponzio
Deputy County Counsel

- | | | |
|---------------------|---|--|
| Attachments: | Exhibit B-6,
Exhibit D-1,
Exhibit E-1,
Exhibit F,
Exhibit G,

Exhibit I, | Price Summary and Compensation Plan
Business Association Agreement
User Responsibility Statement
Remote Access
Contractor Certification Of Compliance With
Covid-19 Vaccine Requirements
Insurance Requirements For Professional
Services Contracts |
|---------------------|---|--|

EXHIBIT B-6

PRICE SUMMARY AND COMPENSATION PLAN

All pricing listed below shall be firm during the term of the Agreement.
Purchase Order is due upon execution of this Amendment for year one. 100% payment due within thirty (30) days receipt of invoice.

County has the option to terminate device module licenses at any time. If the County terminates prior the expiration of the annual license term and if the County has paid a full annual fee, ARDx Informatics will provide a prorated refund for any portion of the unused license term.
County has the option to purchase additional modules at the then-current pricing.

PO/Billing will be made on annual basis at 1/5th total cost of 5 year service contract, between customer and distributor and service provider at \$97,783.08 per year.
All invoices are net thirty (30) days receipt of invoice.

Abbott Rapid Diagnostics Informatics, Inc.			
RALS™		www.rals.com	
Connectivity without Limits™		2000 Holiday Drive, Suite 500, Charlottesville, VA 22901	
		General Information: 1.888.971.7953	
		Customer Support: 1.877.627.7257	
		Fax: 866-533-9071 Email: InformaticsSales@abbott.com	
County of Santa Clara			
San Jose, CA 95131			
Santa Clara Valley Medical Center	San Jose, CA	O'Conner Hospital	San Jose, CA
Saint Louise Regional Hospital	Gilroy, CA		
System Information			
Product:	RALS-Web3	Date:	1/23/2022
Customer #:	A#-00000947	AI Executive:	Mike McNamara
RCS #:	RCS-1879	RAM:	Beth Butler
AI Contract #:		Fax #:	866-533-9071
		Email:	InformaticsSales@abbott.com
Device Module	Quote#		5 Year License Total
Abbott ID NOW™ module	815-012302-022 A	Renewal	\$ 46,765.35
HemoCue® 201 DM HB Module	815-012305-022 A	Renewal	\$ 48,855.15
IL AVOXimeter® 1000E Module	815-012303-022 A	Renewal	\$ 38,523.60
Medtronic ACT® Plus Module	815-012304-022 A	Renewal	\$ 46,834.20
Medtronic Hepcon HMS™ Plus Module	815-012306-022 A	Renewal	\$ 42,678.90
Roche ACCU-CHEK® Inform II Module	815-012301-022 A	Renewal	\$ 156,216.00
Siemens DCA Vantage® Module	815-012309-022 A	Renewal	\$ 50,989.50
RALS eQUIZ			
eQUIZ	815-012307-022 A	Renewal	\$ 26,860.00
Other Components & Services			
Level II Test System & Support	815-012308-022 A	Renewal	\$ 6,305.00
Manual Test Entry (MTE)	815-012310-022 A	New Module	\$19,371.10
Total License Fees:			\$483,398.80
The Technology License includes service, support, and updates maintenance. The supply of RALS for use by Customer is governed by the terms and conditions of the RALS Software System and Support Master Agreement. <i>Please make all purchase orders out to Abbott Rapid Diagnostics Informatics, Inc. Thank you.</i>			
The above offering of products, services and prices will remain in effect until:			December 31, 2021

Abbott Rapid Diagnostics Informatics, Inc.
RALS™

www.rals.com

2000 Holiday Drive, Suite 500, Charlottesville, VA 22901

General Information: 1.888.971.7953

Customer Support: 1.877.627.7257

Fax: 866-533-9071 Email: informaticsSales@abbott.com

Connectivity without Limits™

County of Santa Clara
 San Jose, CA 95131

Santa Clara Valley Medical Center	San Jose, CA	O'Conner Hospital	San Jose, CA
Saint Louise Regional Hospital	Gilroy, CA		

System Information			
Product:	RALS-Web3	Quote #:	815-012301-022 A
Customer #:	A#-00000947	Opportunity #:	O-012122 55528
RCS #:	RCS-1879	AI Contract #:	00004473
LIIS Vendor:		Project Start Date:	
VHOST Required:		Project Go Live Date:	
		Date:	January 23, 2022
		AI Executive:	Mike McNamara
		RAM:	Beth Butler
		Fax #:	866-533-9071
		Email:	informaticsSales@abbott.com
License Term Years:	5.00	Effective/Expire Date:	7/10/2022 - 7/9/2027

MODULE CHARGE
(Includes up to 5 sites per full module charge. If all 5 facilities are implemented within 90 days of the first facility go-live, web remote access capabilities, HL7 results interface, ADT in-hospital patient verification) **each additional facility add after initial 5 sites per full module charge will be at 1/3 of full price module fee.

Device	QTY	Annual Pricing
Roche ACCU-CHEK® Inform II Module	1	\$3,208.00
Meters / Instruments / Analyzers:		
Total number of Meters / Instruments / Analyzers:	293	\$28,421.00
SCVMC/Custody	211	
O'Connor	63	
Saint Louise	19	
System Support Model	Y	Incl. With Module
RALS Silver Support Tier	Y	Incl. With Module
RALS-Web3 Browser Based Remote Access		
# Hospitals Using Web:	3	Incl. With Module
Results Interface		
LIIS HL7 Un-Solicited Results	1	(1) HL7 LIIS INTF Incl. With Module*
ADT Interface (admit, discharge, transfer)		(1) in Hospital ADT Incl. With Module**
ADT In-Unit Patient Verification w/PPI (Positive Patient Identification)	1	\$1,341.00
*HL7 LIIS INTF Incl. With Module if completed within 30 days of GO LIVE.		
** Additional LIIS and ADT interfaces at extra cost (i.e. solicited vs. unsolicited results)		
Module Charge and Interfacing SUB-TOTAL:		\$38,970.00

LICENSE TERM COST AND DISCOUNTS		
Total Annual License Cost Basis:	\$38,970.00	License Term Years: 5
License Total (entire term, before discounts):		\$194,850.00
Less: 10% Discount for 5+ year Annualized Pay	Y	-\$19,485.00
		License Subtotal After Discount
		\$175,365.00
Less: One Time Approved 10% Customer Discount	Y	-\$17,536.50
		License Subtotal After Discount
		\$157,828.50
Less: One Time Approved Customer Discount	Y	-\$1,612.50
		License Subtotal After Discount
		\$156,216.00
LICENSE TOTAL (entire term after discounts):		\$156,216.00

*This quote is valid for work performed during normal business hours of Monday through Friday, 7AM - 7PM eastern time, excluding holidays. Additional fees apply for work performed outside these hours.

Total Contract Amount for License/Implementation/Training* \$156,216.00
 ** Plus Applicable Sales Tax (if non-applicable please submit Exemption Cert)

Annualized Payments Schedule			
Year	Payor		Due:
One	Customer Pay		\$31,243.20
Two	Customer Pay		\$31,243.20
Three	Customer Pay		\$31,243.20
Four	Customer Pay		\$31,243.20
Five	Customer Pay		\$31,243.20
Total Contract Amount for License/Implementation/Training*			\$156,216.00

The supply of RALS for use by Customer is governed by the terms and conditions of the RALS Software System and Support Master Agreement. Notwithstanding the foregoing, additional meters, LIIS and/or ADT upgrades, additional interface services, and any services as defined in the Master Agreement to the existing License Software Module referenced above ("Additional Services") shall be deemed incorporated into the RALS Software System and Support Master Agreement, until the License Agreement Term End Date. For the sake of clarity, Customer acknowledges and agrees that it shall pay ARDx informatics for any costs associated with the Additional Services. Please make all purchase orders out to Abbott Rapid Diagnostics Informatics, Inc. Thank you.

The above offering of products, services and prices will remain in effect until: **December 31, 2022**

**Abbott Rapid Diagnostics Informatics, Inc.
RALS™**

www.rals.com

2000 Holiday Drive, Suite 500, Charlottesville, VA 22901

General Information: 1.888.971.7953

Customer Support: 1.877.627.7257

Fax: 866-533-9071 Email: informaticsSales@abbott.com

Connectivity without Limits™

County of Santa Clara			
San Jose, CA 95131			
Santa Clara Valley Medical Center	San Jose, CA	O'Conner Hospital	San Jose, CA
System Information			
Product:	RALS-Web3	Quote #:	815-012302-022 A
Customer #:	A#-00000947	Opportunity #:	O-012122 55529
RC# #:	RC#-1879	AI Contract #:	00018553
LI# Vendor:		Project Start Date:	
VHOST Required:		Project Go Live Date:	
License Term Years:	5.00	Effective/Expire Date:	7/10/2022 - 7/9/2027

MODULE CHARGE		
<small>(*Includes up to 3 sites per full module charge, if all 3 facilities are implemented within 90 days of the first facility go-live, web remote access capabilities, HL7 results interface, ADT in-hospital patient verification) **Each additional facility add after initial 3 sites per full module charge will be at 1/3 of full price module fee</small>		
Device	QTY	Annual Pricing
Abbott ID NOW™ module	1	\$8,627.00
Meters / Instruments / Analyzers:		
Total number of Meters / Instruments / Analyzers:	9	\$3,033.00
SCVMC/Custody O'Connor	7 2	
System Support Model	Y	Incl. With Module
RALS Silver Support Tier	Y	Incl. With Module
RALS-Web3 Browser Based Remote Access		
# Hospitals Using Web:	2	Incl. With Module
Results Interface		
LIS HL7 Un-Solicited Results	1	(1) HL7 LIS INTF Incl. With Module*
<small>*HL7 LIS INTF Incl. With Module if completed within 30 days of GO LIVE. ** Additional LIS and ADT interfaces at extra cost (i.e. solicited vs. unsolicited results)</small>		
Module Charge and Interfacing SUB-TOTAL:		\$11,660.00

LICENSE TERM COST AND DISCOUNTS		
Total Annual License Cost Basis:	\$11,660.00	License Term Years: 5
License Total (entire term, before discounts):		\$58,300.00
Less: 10% Discount for 5+ year Annualized Pay	Y	-\$5,830.00
		License Subtotal After Discount
		\$52,470.00
Less: One Time Approved 10% Customer Discount	Y	-\$5,247.00
		License Subtotal After Discount
		\$47,223.00
Less: One Time Approved Customer Discount	Y	-\$457.65
		License Subtotal After Discount
		\$46,765.35
LICENSE TOTAL (entire term after discounts):		\$46,765.35

*This quote is valid for work performed during normal business hours of Monday through Friday, 7AM - 7PM eastern time, excluding holidays. Additional fees apply for work performed outside these hours.

Total Contract Amount for License/Implementation/Training* **\$46,765.35**

Plus Applicable Sales Tax (if non-applicable please submit Exemption Cert)

Annualized Payments Schedule			
Year	Payor		Due:
One	Customer Pay		\$9,353.07
Two	Customer Pay		\$9,353.07
Three	Customer Pay		\$9,353.07
Four	Customer Pay		\$9,353.07
Five	Customer Pay		\$9,353.07
Total Contract Amount for License/Implementation/Training*			\$46,765.35

The supply of RALS for use by Customer is governed by the terms and conditions of the RALS Software System and Support Master Agreement. Notwithstanding the foregoing, additional meters, LIS and/or ADT upgrades, additional interface services, and any services as defined in the Master Agreement to the existing License Software Module referenced above ("Additional Services") shall be deemed incorporated into the RALS Software System and Support Master Agreement until the License Agreement Term End Date. For the sake of clarity, Customer acknowledges and agrees that it shall pay ARDX Informatics for any costs associated with the Additional Services. Please make all purchase orders out to Abbott Rapid Diagnostics Informatics, Inc. Thank you.

The above offering of products, services and prices will remain in effect until: **December 31, 2022**

Abbott Rapid Diagnostics Informatics, Inc.
RALS™

www.rals.com

2000 Holiday Drive, Suite 500, Charlottesville, VA 22901

General Information: 1.888.971.7953

Customer Support: 1.877.627.7257

Fax: 866-533-9071 Email: informaticsSales@abbott.com

Connectivity without Limits™

County of Santa Clara			
San Jose, CA 95131			
O'Connor Hospital		San Jose, CA	
System Information			
Product:	RALS-Web3	Quote #:	815-012303-022 A
Customer #:	A#-00000947	Opportunity #:	O-012322 55540
RCS #:	RCS-1879	AI Contract #:	00012361
LIS Vendor:		Project Start Date:	
VHOST Required:		Project Go Live Date:	
AI Executive:	Mike McNamara	RAM:	Beth Butler
Fax #:	866-533-9071	Email:	informaticsSales@abbott.com
License Term Years:	5.00	Effective/Expire Date:	7/10/2022 - 7/9/2027

MODULE CHARGE		
(Includes up to 3 sites per full module charge, if all 3 facilities are implemented within 90 days of the first facility go-live, web remote access capabilities, HL7 results interface, ADT in-hospital patient verification) **each additional facility add after initial 3 sites per full module charge will be at 10% of full price module fee		
Device	QTY	Annual Pricing
IL AVOXimeter® 1000E Module	<input type="text" value="1"/>	\$8,916.00
Meters / Instruments / Analyzers:		
Total number of Meters / Instruments / Analyzers:	<input type="text" value="2"/>	\$690.00
System Support Model	<input type="text" value="Y"/>	Incl. With Module
RALS Silver Support Tier	<input type="text" value="Y"/>	Incl. With Module
RALS-Web3 Browser Based Remote Access		
# Hospitals Using Web:	<input type="text" value="1"/>	Incl. With Module
Results Interface		
LIS HL7 Un-Solicited Results	<input type="text" value="1"/>	(1) HL7 LIS INTF Incl. With Module*
*HL7 LIS INTF Incl. With Module if completed within 90 days of GO LIVE. ** Additional LIS and ADT interfaces at extra cost (i.e. solicited vs. unsolicited results)		
Module Charge and Interfacing SUB-TOTAL:		\$9,606.00

LICENSE TERM COST AND DISCOUNTS		
Total Annual License Cost Basis:	\$9,606.00	License Term Years: 5
License Total (entire term, before discounts):		\$48,030.00
Less: 10% Discount for 5+ year Annualized Pay	<input type="text" value="Y"/>	-\$4,803.00
License Subtotal After Discount		\$43,227.00
Less: One Time Approved 10% Customer Discount	<input type="text" value="Y"/>	-\$4,322.70
License Subtotal After Discount		\$38,904.30
Less: One Time Approved Customer Discount	<input type="text" value="Y"/>	-\$380.70
License Subtotal After Discount		\$38,523.60
LICENSE TOTAL (entire term after discounts):		\$38,523.60

**This quote is valid for work performed during normal business hours of Monday through Friday, 7AM - 7PM eastern time, excluding holidays. Additional fees apply for work performed outside these hours.*

Total Contract Amount for License/Implementation/Training*	\$38,523.60
<i>* Plus Applicable Sales Tax (if non-applicable please submit Exemption Cert)</i>	

Annualized Payments Schedule			
Year	Payor	Due:	
One	Customer Pay	\$7,704.72	
Two	Customer Pay	\$7,704.72	
Three	Customer Pay	\$7,704.72	
Four	Customer Pay	\$7,704.72	
Five	Customer Pay	\$7,704.72	
Total Contract Amount for License/Implementation/Training*		\$38,523.60	

The supply of RALS for use by Customer is governed by the terms and conditions of the RALS Software System and Support Master Agreement. Notwithstanding the foregoing, additional meters, LIS and/or ADT upgrades, additional interface services, and any services as defined in the Master Agreement to the existing License Software Module referenced above ("Additional Services") shall be deemed incorporated into the RALS Software System and Support Master Agreement, until the License Agreement Term End Date. For the sake of clarity, Customer acknowledges and agrees that it shall pay ARDI Informatics for any costs associated with the Additional Services. Please make all purchase orders out to Abbott Rapid Diagnostic Informatics, Inc. Thank you.

The above offering of products, services and prices will remain in effect until: **December 31, 2022**

Abbott Rapid Diagnostics Informatics, Inc. RALS™		www.rals.com	
		2000 Holiday Drive, Suite 500, Charlottesville, VA 22801	
Connectivity without Limits™		General Information: 1.888.971.7953	
		Customer Support: 1.877.627.7257	
		Fax: 866-533-9071 Email: informaticsSales@abbott.com	
County of Santa Clara			
San Jose, CA 95131			
O'Connor Hospital		San Jose, CA	
System Information			
Product:	RALS-Web3	Quote #:	815-012304-022 A
Customer #:	A#-00000947	Opportunity #:	O-012322 55541
RCS #:	RCS-1879	AI Contract #:	00016122
LIS Vendor:		Project Start Date:	
VHOST Required:		Project Go Live Date:	
AI Executive:	Mike McNamara	RAM:	Beth Butler
		Fax #:	866-533-9071
		Email:	informaticsSales@abbott.com
License Term Years:	5.00	Effective/Expire Date:	7/10/2022 - 7/9/2027
MODULE CHARGE			
<small>(*Includes up to 3 sites per full module charge, if all 3 facilities are implemented within 90 days of the first facility go-live, web remote access capabilities, HL7 results interface, ADT in-hospital patient verification) **each additional facility add after initial 3 sites per full module charge will be at 1/3 of full price module fee</small>			
Device	QTY	Annual Pricing	
Medtronic ACT® Plus Module	1	\$8,916.00	
Meters / Instruments / Analyzers:			
Total number of Meters / Instruments / Analyzers:	8	\$2,760.00	
System Support Model	Y	Incl. With Module	
RALS Silver Support Tier	Y	Incl. With Module	
RALS-Web3 Browser Based Remote Access			
# Hospitals Using Web:	1	Incl. With Module	
Results Interface			
LIS HL7 Un-Solicited Results	1	(1) HL7 LIS INTF Incl. With Module*	
<small>*HL7 LIS INTF Incl. With Module If completed within 30 days of GO LIVE. ** Additional LIS and ADT Interfaces at extra cost (i.e. solicited vs. unsolicited results)</small>			
Module Charge and Interfacing SUB-TOTAL:			\$11,676.00
LICENSE TERM COST AND DISCOUNTS			
Total Annual License Cost Basis:	\$11,676.00	License Term Years:	5
License Total (entire term, before discounts):			\$58,380.00
Less: 10% Discount for 5+ year Annualized Pay	Y		-\$5,838.00
		License Subtotal After Discount	\$52,542.00
Less: One Time Approved 10% Customer Discount	Y		-\$5,254.20
		License Subtotal After Discount	\$47,287.80
Less: One Time Approved Customer Discount	Y		-\$453.60
		License Subtotal After Discount	\$46,834.20
LICENSE TOTAL (entire term after discounts):			\$46,834.20
<small>*This quote is valid for work performed during normal business hours of Monday through Friday, 7AM - 7PM eastern time, excluding holidays. Additional fees apply for work performed outside these hours.</small>			
Total Contract Amount for License/Implementation/Training*			\$46,834.20
<small>* Plus Applicable Sales Tax (if non-applicable please submit Exemption Cert)</small>			
Annualized Payments Schedule			
	Year	Payor	Due:
	One	Customer Pay	\$9,366.84
	Two	Customer Pay	\$9,366.84
	Three	Customer Pay	\$9,366.84
	Four	Customer Pay	\$9,366.84
	Five	Customer Pay	\$9,366.84
Total Contract Amount for License/Implementation/Training*			\$46,834.20
<p>The supply of RALS for use by Customer is governed by the terms and conditions of the RALS Software System and Support Master Agreement. Notwithstanding the foregoing, additional meters, LIS and/or ADT upgrades, additional interface services, and any services as defined in the Master Agreement to the existing License Software Module referenced above ("Additional Services") shall be deemed incorporated into the RALS Software System and Support Master Agreement, until the License Agreement Term End Date. For the sake of clarity, Customer acknowledges and agrees that it shall pay ARDx Informatics for any costs associated with the Additional Services.</p> <p>Please make all purchase orders out to Abbott Rapid Diagnostic Informatics, Inc. Thank you.</p>			
The above offering of products, services and prices will remain in effect until:			December 31, 2022

Abbott Rapid Diagnostics Informatics, Inc.
RALS™

www.rals.com

2000 Holiday Drive, Suite 500, Charlottesville, VA 22901

Connectivity without Limits™

General Information: 1.888.971.7953

Customer Support: 1.877.627.7257

Fax: 866-533-9071 Email: informaticsSales@abbott.com

County of Santa Clara			
San Jose, CA 95131			
O'Connor Hospital		San Jose, CA	
System Information			
Product:	RALS-Web3	Quote #:	815-012305-022 A
Customer #:	A#-00000947	Opportunity #:	O-012322 55542
RCS #:	RCS-1879	AI Contract #:	00018043
LIS Vendor:		Project Start Date:	
VHOST Required:		Project Go Live Date:	
AI Executive:		RAM:	Beth Butler
		Fax #:	866-533-9071
		Email:	informaticsSales@abbott.com
License Term Years:	5.00	Effective/Expires Date:	7/10/2022 - 7/9/2027

MODULE CHARGE		
<small>(Includes up to 3 sites per full module charge, if all 3 facilities are implemented within 90 days of the first facility go-live, with remote access capabilities, HL7 results interface, ADT in-hospital patient verification) *Each additional facility add after initial 3 sites per full module charge will be at 1/3 of full price module fee</small>		
Device	QTY	Annual Pricing
HemoCue® 201 DM HB Module	1	\$11,492.00
Meters / Instruments / Analyzers:		
Total number of Meters / Instruments / Analyzers:	2	\$690.00
System Support Model	Y	Incl. With Module
RALS Silver Support Tier	Y	Incl. With Module
RALS-Web3 Browser Based Remote Access		
# Hospitals Using Web:	1	Incl. With Module
Results Interface		
LIS HL7 Un-Solicited Results	1	(1) HL7 LIS INTF Incl. With Module*
<small>*HL7 LIS INTF Incl. With Module if completed within 90 days of GO LIVE. ** Additional LIS and ADT Interfaces at extra cost (i.e. solicited vs. unsolicited results)</small>		
Module Charge and Interfacing SUB-TOTAL:		\$12,182.00

LICENSE TERM COST AND DISCOUNTS		
Total Annual License Cost Basis:	\$12,182.00	License Term Years: 5
License Total (entire term, before discounts):		\$60,910.00
Less: 10% Discount for 5+ year Annualized Pay	Y	\$6,091.00
		License Subtotal After Discount
		\$54,819.00
Less: One Time Approved 10% Customer Discount	Y	\$5,481.90
		License Subtotal After Discount
		\$49,337.10
Less: One Time Approved Customer Discount	Y	\$49,337.10
		License Subtotal After Discount
		\$48,855.15
LICENSE TOTAL (entire term after discounts):		
\$48,855.15		

*This quote is valid for work performed during normal business hours of Monday through Friday, 7AM - 7PM eastern time, excluding holidays. Additional fees apply for work performed outside these hours.

Total Contract Amount for License/Implementation/Training*	\$48,855.15
<small>* Plus Applicable Sales Tax (if non-applicable please submit Exemption Cert)</small>	

Annualized Payments Schedule			
Year	Payor		Due:
One	Customer Pay		\$9,771.03
Two	Customer Pay		\$9,771.03
Three	Customer Pay		\$9,771.03
Four	Customer Pay		\$9,771.03
Five	Customer Pay		\$9,771.03
Total Contract Amount for License/Implementation/Training*			\$48,855.15

The supply of RALS for use by Customer is governed by the terms and conditions of the RALS Software System and Support Master Agreement. Notwithstanding the foregoing, additional meters, LIS and/or ADT upgrades, additional interface services, and any services as defined in the Master Agreement to the existing License Software Module referenced above ("Additional Services") shall be deemed incorporated into the RALS Software System and Support Master Agreement, until the License Agreement Term End Date. For the sake of clarity, Customer acknowledges and agrees that it shall pay ARDx Informatics for any costs associated with the Additional Services. Please make all purchase orders out to Abbott Rapid Diagnostics Informatics, Inc. Thank you.

The above offering of products, services and prices will remain in effect until: **December 31, 2022**

Abbott Rapid Diagnostics Informatics, Inc.
RALS™

www.rals.com

2000 Holiday Drive, Suite 500, Charlottesville, VA 22901

Connectivity without Limits™

General Information: 1.888.971.7953

Customer Support: 1.877.627.7257

Fax: 866-533-9071 Email: informaticsSales@abbott.com

County of Santa Clara					
San Jose, CA 95131					
Santa Clara Valley Medical Center		San Jose, CA			
System Information					
Product:	RALS-Web3	Quote #:	815-012306-022 A	Date:	January 23, 2022
Customer #	A#-00000947	Opportunity #:	O-012322 55543	AI Executive:	Mike McNamara
RCS #:	RCS-1879	AI Contract #:	00011545	RAM:	Beth Butler
LIS Vendor:		Project Start Date:		Fax #:	866-533-9071
VHOST Required:		Project Go Live Date:		Email:	informaticsSales@abbott.com
License Term Years:	5.00	Effective/Expire Date:	7/10/2022 - 7/9/2027		

MODULE CHARGE		
<small>(*Includes up to 3 sites per full module charge, if all 3 facilities are implemented within 90 days of the first facility go-live, web remote access capabilities, HL7 results interface, ADT in-hospital patient verification) **Each additional facility add after initial 3 sites per full module charge will be at 1/3 of full price module fee</small>		
Device	QTY	Annual Pricing
Medtronic Hepcon HMS™ Plus Module	<input type="text" value="1"/>	\$8,916.00
Meters / Instruments / Analyzers:		
Total number of Meters / Instruments / Analyzers:	<input type="text" value="5"/>	\$1,725.00
System Support Model	<input type="text" value="Y"/>	Incl. With Module
RALS Silver Support Tier	<input type="text" value="Y"/>	Incl. With Module
RALS-Web3 Browser Based Remote Access		
# Hospitals Using Web:	<input type="text" value="1"/>	Incl. With Module
Results Interface		
LIS HL7 Un-Solicited Results	<input type="text" value="1"/>	(1) HL7 LIS INTF Incl. With Module*
<small>*HL7 LIS INTF Incl. With Module If completed within 90 days of GO LIVE. ** Additional LIS and ADT interfaces at extra cost (i.e. solicited vs. unsolicited results)</small>		
Module Charge and Interfacing SUB-TOTAL:		\$10,641.00

LICENSE TERM COST AND DISCOUNTS		
Total Annual License Cost Basis:	\$10,641.00	License Term Years: 5
License Total (entire term, before discounts):		\$53,205.00
Less: 10% Discount for 5+ year Annualized Pay	<input type="text" value="Y"/>	-\$5,320.50
		License Subtotal After Discount
		\$47,884.50
Less: One Time Approved 10% Customer Discount	<input type="text" value="Y"/>	-\$4,788.45
		License Subtotal After Discount
		\$43,096.05
Less: One Time Approved Customer Discount	<input type="text" value="Y"/>	-\$417.15
		License Subtotal After Discount
		\$42,678.90
LICENSE TOTAL (entire term after discounts):		\$42,678.90

*This quote is valid for work performed during normal business hours of Monday through Friday, 7AM - 7PM eastern time, excluding holidays. Additional fees apply for work performed outside these hours.

Total Contract Amount for License Implementation/Training* \$42,678.90
* Plus Applicable Sales Tax (if non-applicable please submit Exemption Cert)

Annualized Payments Schedule			
Year	Payor		Due:
One	Customer Pay		\$8,535.78
Two	Customer Pay		\$8,535.78
Three	Customer Pay		\$8,535.78
Four	Customer Pay		\$8,535.78
Five	Customer Pay		\$8,535.78
Total Contract Amount for License Implementation/Training*			\$42,678.90

The supply of RALS for use by Customer is governed by the terms and conditions of the RALS Software System and Support Master Agreement. Notwithstanding the foregoing, additional meters, LIS and/or ADT upgrades, additional interface services, and any services as defined in the Master Agreement to the existing License Software Module referenced above ("Additional Services") shall be deemed incorporated into the RALS Software System and Support Master Agreement, until the License Agreement Term End Date. For the sake of clarity, Customer acknowledges and agrees that it shall pay ARDx Informatics for any costs associated with the Additional Services.
 Please make all purchase orders out to Abbott Rapid Diagnostic Informatics, Inc. Thank you.

The above offering of products, services and prices will remain in effect until: December 31, 2022

Abbott Rapid Diagnostics Informatics, Inc.
RALS™

www.rals.com

2000 Holiday Drive, Suite 500, Charlottesville, VA, 22901

Connectivity without Limits™

General Information: 1.888.971.7953

Customer Support: 1.877.627.7257

Fax: 866-533-9071 Email: informaticsSales@abbott.com

County of Santa Clara			
San Jose, CA 95131			
Santa Clara Valley Medical Center	San Jose, CA	O'Conner Hospital	San Jose, CA
Saint Louise Regional Hospital	Gilroy, CA		
System Information			
Product:	RALS-Web3	Quote #:	815-012307-022 A
Customer #	A#-00000947	Opportunity #:	O-012322 55544
RCS #:	RCS-1879	AI Contract #:	00013513
LIS Vendor:		Project Start Date:	
VHOST Required:		Project Go Live Date:	
	License Term Years:	5.00	EMR/CDM/Expires Date:
			7/10/2022 - 7/9/2027
RALS eQuiz			
			Pricing
Total Operators (Minimum \$1,000 per year)		5372	\$5,372.00
Santa Clara Valley		2972	
O'Connor		1600	
Saint Louise		800	
ADDITIONAL COMPONENTS SUB-TOTAL:			\$5,372.00
LICENSE TOTAL:			\$26,860.00
Total Contract Amount for License/Installation/Training*			\$26,860.00
<i>* Plus Applicable Sales Tax (if non-applicable please submit Exemption Cert)</i>			
Annualized Payments Schedule			
	Year	Payor	Due:
	One	Customer Pay	\$5,372.00
	Two	Customer Pay	\$5,372.00
	Three	Customer Pay	\$5,372.00
	Four	Customer Pay	\$5,372.00
	Five	Customer Pay	\$5,372.00
<p>The supply of RALS for use by Customer is governed by the terms and conditions of the RALS Software System and Support Master Agreement. Notwithstanding the foregoing, additional meters, LIS and/or ADT upgrades, additional interface services, and any services as defined in the Master Agreement to the existing License Software Module referenced above ("Additional Services") shall be deemed incorporated into the RALS Software System and Support Master Agreement, until the License Agreement Term End Date. For the sake of clarity, Customer acknowledges and agrees that it shall pay ARDx Informatics for any costs associated with the Additional Services. Please make all purchase orders out to Abbott Rapid Diagnostic Informatics, Inc. Thank you.</p>			
The above offering of products, services and prices will remain in effect until: December 31, 2022			

Abbott Rapid Diagnostics Informatics, Inc. RALS™ Connectivity without Limits™		www.rals.com 2000 Holiday Drive, Suite 500, Charlottesville, VA 22901 General Information: 1.888.971.7953 Customer Support: 1.877.627.7257 Fax: 966-533-9071 Email: informaticsSales@abbott.com	
County of Santa Clara San Jose, CA 95131			
Santa Clara Valley Medical Center	San Jose, CA	O'Connor Hospital	San Jose, CA
Saint Louise Regional Hospital	Gilroy, CA		
System Information			
Product:	RALS-Web3	Quote #:	815-012308-022 A
Customer #:	A#-00000947	Opportunity #:	O-012322 55545
RCS #:	RCS-4275	AI Contract #:	00011830
LIS Vendor:		Project Start Date:	
VHOST Required:		Project Go Live Date:	
License Term Years:	5.00	Effective/Expire Date:	7/10/2022 - 7/9/2027
LICENSE COSTS			
RALS Test Area/System Annual Support & Maintenance	5	years support	\$6,370.00
Less: One Time Approved Customer Discount	Y		-\$65.00
LICENSE TOTAL:			\$6,305.00
<i>*This quote is valid for work performed during normal business hours of Monday through Friday, 7AM – 7PM eastern time, excluding holidays. Additional fees apply for work performed outside these hours.</i>			
Total Contract Amount for License/Implementation/Training*			\$6,305.00
<i>* Plus Applicable Sales Tax (if non-applicable please submit Exemption Cert)</i>			
Annualized Payments Schedule			
	Year	Payor	Due:
	One	Customer Pay	\$1,261.00
	Two	Customer Pay	\$1,261.00
	Three	Customer Pay	\$1,261.00
	Four	Customer Pay	\$1,261.00
	Five	Customer Pay	\$1,261.00
Total Contract Amount for License/Implementation/Training*			\$6,305.00
The supply of RALS for use by Customer is governed by the terms and conditions of the RALS Software System and Support Master Agreement. Notwithstanding the foregoing, additional meters, LIS and/or ADT upgrades, additional interface services, and any services as defined in the Master Agreement to the existing License Software Module referenced above ("Additional Services") shall be deemed incorporated into the RALS Software System and Support Master Agreement until the License Agreement Term End Date. For the sake of clarity, Customer acknowledges and agrees that it shall pay ARDx Informatics for any costs associated with the Additional Services. Please make all purchase orders out to Abbott Rapid Diagnostic Informatics, Inc. Thank you.			
The above offering of products, services and prices will remain in effect until:			December 31, 2021

Abbott Rapid Diagnostics Informatics, Inc.
RALS™

www.rals.com

2000 Holiday Drive, Suite 500, Charlottesville, VA 22901

Connectivity without Limits™

General Information: 1.888.971.7953

Customer Support: 1.877.627.7257

Fax: 866-533-9071 Email: informaticsSales@abbott.com

Santa Clara Valley Medical Center

San Jose, CA 95128

System Information

Product:	RALS-Web3	Quote #:	815-012309-022 A	Date:	October 21, 2021
Customer #:	A#-00000947	Opportunity #:	O-012322 55546	AI Executive:	Mike McNamara
RCS #:	RCS-1879	AI Contract #:	00020771	RAM:	Beth Butler
LIS Vendor:		Project Start Date:		Fax #:	866-533-9071
VHOST Required:		Project Go Live Date:		Email:	informaticsSales@abbott.com
License Term Years:	5.00	Effective/Expire Date:	7/10/2022 - 7/9/2027		

MODULE CHARGE

(Includes up to 3 sites per full module charge. If all 3 facilities are implemented within 90 days of the first facility go-live, web remote access capabilities, HL7 results interface, ADT in-hospital patient verification) *Each additional facility add after initial 3 sites per full module charge will be at 1/3 of full price module fee

Device	QTY	Annual Pricing
Siemens Healthineers DCA Vantage® Module	1	\$8,516.00
Meters / Instruments / Analyzers:		
Total number of Meters / Instruments / Analyzers:	11	\$3,795.00
System Support Model	Y	Incl. With Module
RALS Silver Support Tier	Y	Incl. With Module
RALS-Web3 Browser Based Remote Access		
# Hospitals Using Web:	1	Incl. With Module
Results Interface		
LIS HL7 Un-Solicited Results	1	(1) HL7 LIS INTF Incl. With Module*

*HL7 LIS INTF Incl. With Module If completed within 90 days of GO LIVE.
 ** Additional LIS and ADT Interfaces at extra cost (i.e. solicited vs. unsolicited results)

Module Charge and Interfacing SUB-TOTAL: **\$12,711.00**

LICENSE TERM COST AND DISCOUNTS

Total Annual License Cost Basis:	\$12,711.00	License Term Years:	5
License Total (entire term, before discounts):			\$63,555.00
Less: 10% Discount for 5+ year Annualized Pay	Y		-\$6,355.50
License Subtotal After Discount			\$57,199.50
Less: One Time Approved 10% Customer Discount	Y		-\$5,719.95
License Subtotal After Discount			\$51,479.55
Less: One Time Approved Customer Discount	Y		-\$490.05
License Subtotal After Discount			\$50,989.50
LICENSE TOTAL (entire term after discounts):			\$50,989.50

*This quote is valid for work performed during normal business hours of Monday through Friday, 7AM - 7PM eastern time, excluding holidays. Additional fees apply for work performed outside these hours.

Total Contract Amount for License/Implementation/Training* **\$50,989.50**

* Plus Applicable Sales Tax (if non-applicable please submit Exemption Cert)

Annualized Payments Schedule

Year	Payor	Due:
One	Customer Pay	\$10,197.90
Two	Customer Pay	\$10,197.90
Three	Customer Pay	\$10,197.90
Four	Customer Pay	\$10,197.90
Five	Customer Pay	\$10,197.90
Total Contract Amount for License/Implementation/Training*		\$50,989.50

The supply of RALS for use by Customer is governed by the terms and conditions of the RALS Software System and Support Master Agreement. Notwithstanding the foregoing, additional meters, LIS and/or ADT upgrades, additional interface services, and any services as defined in the Master Agreement to the existing License Software Module referenced above ("Additional Services") shall be deemed incorporated into the RALS Software System and Support Master Agreement, until the License Agreement Term End Date. For the sake of clarity, Customer acknowledges and agrees that it shall pay ARDx informatics for any costs associated with the Additional Services.
 Please make all purchase orders out to Abbott Rapid Diagnostics Informatics, Inc. Thank you.

The above offering of products, services and prices will remain in effect until: **December 31, 2022**

Abbott Rapid Diagnostics Informatics, Inc. RALS™		www.rals.com	
Connectivity without Limits™		2000 Holiday Drive, Suite 500, Charlottesville, VA 22901	
		General Information: 1.888.971.7953	
		Customer Support: 1.877.627.7257	
		Fax: 866-533-9071 Email: informaticsSales@abbott.com	
County of Santa Clara			
Santa Clara Valley Medical Center			
San Jose, CA 95128			
System Information			
Product:	RALS-Web3	Quote #:	815-012910-022 A
Customer #:	A#-00000947	Opportunity #:	O-102121 54083
RCS #:	RCS-1879	AI Contract #:	00021121
LIS Vendor:		Project Start Date:	
VHOST Required:		Project Go Live Date:	
Date:	October 21, 2021	AI Executive:	Mike McNamara
RAM:	Beth Butler	Fax #:	866-533-9071
Email:	informaticsSales@abbott.com		
License Term Years:	5.00	Effective/Expire Date:	
MODULE CHARGE			
<small>(*Includes up to 3 sites per full module charge. If all 3 facilities are implemented within 90 days of the first facility go-live, web remote access capabilities, HL7 results interface, ADT in-hospital patient verification) **Each additional facility add after initial 3 sites per full module charge will be at 1/3 of full price module fee</small>			
Device	QTY	Annual Pricing	
MTE (Manual Test Entry) Module - unlimited	1	\$4,507.00	
System Support Model	Y	Incl. With Module	
RALS Silver Support Tier	Y	Incl. With Module	
RALS-Web3 Browser Based Remote Access			
# Hospitals Using Web:	1	Incl. With Module	
Results Interface			
LIS HL7 Un-Solicited Results	1	(1) HL7 LIS INTF Incl. With Module*	
<small>*HL7 LIS INTF Incl. With Module if completed within 30 days of GO LIVE. ** Additional LIS and ADT interfaces at extra cost (i.e. solicited vs. unsolicited results)</small>			
Module Charge and interfacing SUB-TOTAL:			\$4,507.00
LICENSE TERM COST AND DISCOUNTS			
<i>Total Annual License Cost Basis:</i>	\$4,507.00	License Term Years:	5
License Total (entire term, before discounts):			\$22,535.00
Less: 10% Discount for 5+ year Annualized Pay	Y		-\$2,253.50
		License Subtotal After Discount	\$20,281.50
Less: One Time Approved 10% Customer Discount	Y		-\$2,028.15
		License Subtotal After Discount	\$18,253.35
Less: One Time Approved Customer Discount	Y		-\$182.25
		License Subtotal After Discount	\$18,071.10
		LICENSE TOTAL (entire term after discounts):	\$18,071.10
IMPLEMENTATION *			
MTE Implementation Fee (up to 5 institutions during initial installation (unlimited tests))	Y		\$1,313.00
Less: One Time Approved Customer Discount	Y		-\$13.00
<small>*This quote is valid for work performed during normal business hours of Monday through Friday, 7AM - 7PM eastern time, excluding holidays. Additional fees apply for work performed outside these hours.</small>			
TOTAL IMPLEMENTATION:			\$1,300.00
Total Contract Amount for License/Implementation/Training*			\$19,371.10
<small>* Plus Applicable Sales Tax (if non-applicable please submit Exemption Cert)</small>			
Annualized Payments Schedule			
	Year	Payor	Due:
	One	Customer Pay	\$4,914.22
	Two	Customer Pay	\$3,614.22
	Three	Customer Pay	\$3,614.22
	Four	Customer Pay	\$3,614.22
	Five	Customer Pay	\$3,614.22
Total Contract Amount for License/Implementation/Training*			\$19,371.10
The supply of RALS for use by Customer is governed by the terms and conditions of the RALS Software System and Support Master Agreement. Notwithstanding the foregoing, additional meters, LIS and/or ADT upgrades, additional interface services, and any services as defined in the Master Agreement to the existing License Software Module referenced above ("Additional Services") shall be deemed incorporated into the RALS Software System and Support Master Agreement, until the License Agreement Term End Date. For the sake of clarity, Customer acknowledges and agrees that it shall pay ARDI Informatics for any costs associated with the Additional Services.			
Please make all purchase orders out to Abbott Rapid Diagnostics Informatics, Inc. Thank you.			
The above offering of products, services and prices will remain in effect until:			December 31, 2022

EXHIBIT D-1
BUSINESS ASSOCIATE AGREEMENT

WHEREAS, the County of Santa Clara (“County” or “Covered Entity”) is a covered entity, as defined in the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), and seeks to disclose certain Protected Health Information (defined below) to Abbott Rapid Diagnostics Informatics, Inc. (“Business Associate”) pursuant to the terms of the Agreement between the Parties to this Business Associate Agreement (BAA); and

WHEREAS, the County is a hybrid entity pursuant to HIPAA performing both covered and non-covered functions; and

WHEREAS, the County of Santa Clara Health System (CSCHS), which is part of the County and is comprised of multiple County Departments, including the Santa Clara Valley Medical Center Hospital and Clinics (SCVMC), O’Connor Hospital (OCH), St. Louise Regional Hospital (SLRH), the Behavioral Health Services Department (BHSD), the County Public Health Department (PHD), the County Custody Health Services Department (CHSD), and the Valley Health Plan (VHP); and

WHEREAS, SCVMC, OCH, SLRH, BHSD, CHSD, VHP, and portions of PHD are a “covered entity” under HIPAA; and

WHEREAS, the Covered Entity and Business Associate intend to protect the privacy and provide for the security of PHI used and disclosed pursuant to this BAA in compliance with HIPAA; the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (the “HITECH Act”), and regulations promulgated thereunder by the U.S. Department of Health and Human Services (collectively, the “HIPAA Regulations”); California Welfare & Institutions Code Section 5328; 42 U.S.C. Section 290dd-2; 42 C.F.R part 2; California Confidentiality of Medical Information Act (Civil Code, §56 et seq.); California Health & Safety Code Section 1280.15; and other applicable laws; and to the extent the Business Associate is to carry out the Covered Entity’s obligation under the Privacy Rule (defined below), the Business Associate must comply with the requirements of the Privacy Rule that apply to the Covered Entity in the performance of such obligation.

WHEREAS, part of the HIPAA Regulations, the Privacy Rule and the Security Rule (both of which are defined below) require covered entities to enter into a contract containing specific requirements with any business associate prior to the disclosure of PHI, as set forth in, but not limited to, Title 45, Sections 164.314(a), 164.502(e), and 164.504(e) of the Code of Federal Regulations (C.F.R.) and contained in this BAA.

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

I. Definitions

Terms used, but not otherwise defined, and terms with initial capital letters in the BAA have the same meaning as defined under HIPAA, the HITECH Act, HIPAA Regulations, and other applicable laws.

Business Associate is a person, organization, or agency other than a workforce member that provides specific functions, activities, or services that involve the use, creation, or disclosure of PHI for, or on behalf of, a HIPAA covered health care component. Examples of business associate functions are activities such as claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, practice management, repricing; and legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

Covered Entity shall have the meaning given to such term under the Privacy Rule and the Security Rule, including, but not limited to, 45 C.F.R. Section 160.103.

Designated Record Set shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.

Electronic Protected Health Information means Protected Health Information that is maintained in or transmitted by electronic media.

Electronic Health Record shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C. Section 17921.

Health Care Operations shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.

Privacy Breach shall mean any acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted or allowed under state or federal privacy laws.

Privacy Rule shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and E.

Protected Health Information or PHI means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present, or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 160.103. Protected Health Information includes Electronic Protected Health Information [45 C.F.R. Sections 160.103, 164.501].

Protected Information shall mean PHI provided by Covered Entity to Business Associate or created or received by Business Associate on the Covered Entity's behalf.

Security Rule shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and C.

Unsecured PHI shall have the meaning given to such term under the HITECH Act and any guidance issued pursuant to such Act including, but not limited to, 42 U.S.C. Section 17932(h)(1) and 45 C.F.R. 164.402.

II. Duties & Responsibilities of Business Associate

a. Permitted Uses. Business Associate shall use Protected Information only for the purpose of performing Business Associate's obligations under the Contract and as permitted or required under the Agreement, or as required by law.

Further, Business Associate shall not use Protected Information in any manner that would constitute a violation of the Privacy Rule, Welfare & Institutions Code Section 5328, 42 C.F.R. Part 2, or the HITECH Act, if so used by Covered Entity. However, Business Associate may use Protected Information (i) for the proper management and administration of Business Associate, (ii) to carry out the legal responsibilities of Business Associate, or (iii) for data aggregation purposes for the Health Care Operations of Covered Entity. [45 C.F.R. Sections 164.502(a)(3), 164.504(e)(2)(ii)(A) and 164.504(e)(4)(i)].

b. Permitted Disclosures. Business Associate shall not disclose Protected Information

except for the purpose of performing Business Associate's obligations under the Agreement and as permitted under the Agreement and this BAA. Business Associate shall not disclose Protected Information in any manner that would constitute a violation of the Privacy Rule, 42 C.F.R., Welfare & Institutions Code Section 5328, or the HITECH Act if so disclosed by Covered Entity. However, Business Associate may disclose Protected Information (i) for the proper management and administration of Business Associate; (ii) to carry out the legal responsibilities of Business Associate; (iii) as required by law; or (iv) for Data Aggregation purposes for the Health Care Operations of Covered Entity. If Business Associate discloses Protected Information obtained pursuant to the Agreement and this BAA to a third party, Business Associate must obtain, prior to making any such disclosure, (i) reasonable written assurances from such third party that such Protected Information will be held confidential as provided pursuant to this BAA and only disclosed as required by law or for the purposes for which it was disclosed to such third party, and (ii) a written agreement from such third party to immediately notify Business Associate of any Privacy Breaches of confidentiality of the Protected Information within twenty-four (24) hours of discovery, to the extent it has obtained knowledge of such Privacy Breach. [42 U.S.C. Section 17932; 45 C.F.R. Sections 164.504(e)(2)(i)-(ii)(A) and 164.504(e)(4)(ii)].

c. Prohibited Uses and Disclosures. Business Associate shall not use or disclose

Protected Information for fundraising or marketing purposes. [42 U.S.C. Section 17936(a) and 45 C.F.R. 164.501]. Business Associate shall not disclose Protected Information to a health plan for payment or health care operations purposes if the individual has requested this special restriction, and has paid out of pocket in full for the health care item or service to which the PHI solely relates. [42 U.S.C. Section 17935(a); 45 C.F.R. Section 164.502(a)(5)(ii)]. Business Associate shall not directly or indirectly receive remuneration in exchange for Protected Information, except with the prior written consent of Covered Entity and as permitted by the HITECH Act. [42 U.S.C. Section 17935(d)(2)]. This prohibition shall not affect payment by Covered Entity to Business Associate for services provided pursuant to the Agreement.

d. Appropriate Safeguards. Business Associate shall implement appropriate administrative, technological, and physical safeguards as are necessary to prevent the use or disclosure of Protected Information other than as permitted by this BAA that reasonably and appropriately protect the confidentiality, integrity, and availability of the Protected Information, and comply, where applicable, with the HIPAA Security Rule with respect to Electronic PHI.

e. Reporting of Improper Access, Use, or Disclosure. Business Associate shall notify Covered Entity within ten (10) business days of any suspected or actual Privacy Breach of Protected Information; any use or disclosure of Protected Information not permitted by the Contract or Addendum; any security incident (i.e., any attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system

operations in any information system) related to Protected Information, and any actual or suspected use or disclosure of data in violation of any applicable federal or state laws by Business Associate or its agents or subcontractors.

Business Associate shall report to CSCHS Ethics, Privacy & Compliance Office in writing any access, use, or disclosure of Protected Information not permitted by the Agreement, this BAA, and any other applicable state or federal law, including, but not limited to 42 U.S.C. Section 17921; 45 C.F.R. Section 164.504(e) (2) (ii) (C); 45 C.F.R. Section 164.308(b); California Health & Safety Code 1280.15, California Confidentiality of Medical Information Act 56.10, California Welfare & Institutions 5328 to the following contacts:

Ethics, Privacy & Compliance Office
County of Santa Clara Health System
2325 Enborg Lane, Suite 290
San Jose, California 95128
Facsimile: (408) 885-6006 Telephone: (408) 885-3794
Email: ComplianceOfficer@hhs.sccgov.org

Notices to Business Associate:

Abbott Laboratories
100 Abbott Park Road
Abbott Park, Illinois 60064-3500
Attn: Risk Management, D-317

and

Abbott Laboratories
Legal Regulatory & Compliance
Dept. 32RA, Bldg. AP6A-2
100 Abbott Park Road
Abbott Park, Illinois 60064
Attn: Counsel for Global Privacy

Privacy Steward – ARDx Informatics
Abbott Rapid Diagnostics Informatics, Inc.
2000 Holiday Drive
Charlottesville, VA 22901
Email: Boni.Boutelle@abbott.com

The Privacy Breach notification shall include, to the extent possible, the following: (1) a brief description of what happened, including the date of the Privacy Breach and the date of the discovery of the Privacy Breach, if known; (2) the location of the breached information; (3) the unauthorized person who used the PHI or to whom the disclosure was made; (4) whether the PHI was actually acquired or viewed; (5) a description of the types of PHI that were involved in the Privacy Breach; (6) safeguards in place prior to the Privacy Breach; (7) actions taken in response to the Privacy Breach; (8) any steps individuals should take to protect themselves from potential harm resulting from the Privacy Breach; (9) a brief description of what the business associate is doing to investigate the Privacy Breach, to mitigate harm to individuals, and to protect against further Privacy Breaches; and (10) contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, and website or postal address. [45 C.F.R. Sections 164.410(c) and 164.404(c)]. Business Associate shall take any action pertaining to such unauthorized disclosure required by applicable federal and state laws and regulations. Business Associate

shall otherwise comply with 45 C.F.R. Section 164.410 with respect to reporting Privacy Breaches of Unsecured PHI. [42 U.S.C. Section 17921; 45 C.F.R. Section 164.504(e)(2)(ii)(C); 45 C.F.R. Section 165.308(b)]

f. Business Associate's Agents and Subcontractors. Business Associate shall ensure

that any agents or subcontractors, to whom it provides Protected Information, agree in writing to the same restrictions and conditions that apply to Business Associate with respect to such PHI and implement the safeguards required by paragraph (II)(d) above with respect to Electronic PHI. [45 C.F.R. Sections 164.502(e)(1)(ii), 164.504(e)(2)(ii)(D) and 164.308(b)]. If Business Associate knows of a pattern of activity or practice of an agent or subcontractor that constitutes a material breach or violation of an agent or subcontractor's obligations under the Contract or Addendum or other arrangement, the Business Associate must take reasonable steps to cure the breach or end the violation. If these steps are unsuccessful, Business Associate shall sanction or terminate the contract or arrangement with agent or subcontractor, if feasible. [45 C.F.R. Section 164.504(e)(1)(iii)]. Business Associate shall provide written notification to Covered Entity of any pattern of activity or practice of a subcontractor or agent that Business Associate believes constitutes a material breach or violation of the agent or subcontractor's obligations under the Contract or Addendum or other arrangement within twenty four (24) hours of discovery and shall meet with Covered Entity to discuss and attempt to resolve the problem as one of the reasonable steps to cure the breach or end the violation.

g. Access to Protected Information. Business Associate shall make Protected Information maintained by Business Associate or its agents or subcontractors in Designated Record Sets available to Covered Entity for inspection and copying within ten (10) days of a request by Covered Entity to enable Covered Entity to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.524. [45 C.F.R. Section 164.504(e)(2)(ii) (E); 42 C.F.R. part 2 and Welfare & Institutions Code Section 5328]. If Business Associate maintains an Electronic Health Record, Business Associate shall provide such information in electronic format to enable Covered Entity to fulfill its obligations under the HITECH Act, including, but not limited to, 42 U.S.C. Section 17935(e)(1). If any individual requests access to PHI directly from Business Associate or its agents or subcontractors, Business Associate shall notify Covered Entity in writing within five (5) days of the request.

h. Electronic PHI. If Business Associate receives, creates, transmits, or maintains Electronic PHI on behalf of Covered Entity, Business Associate will, in addition, do the following:

- (1) Develop, implement, maintain, and use appropriate administrative, physical, and technical safeguards in compliance with Section 1173(d) of the Social Security Act, Title 42, Section 1320(s) or the United States Code and Title 45, Part 162 and 164 of CFR to preserve the integrity and confidentiality of all electronically maintained or transmitted PHI received from or on behalf of Covered Entity.
- (2) Document and keep these security measures current and available for inspection by Covered Entity.
- (3) Ensure that any agent, including a subcontractor, to whom the Business Associate provides Electronic PHI, agrees to implement reasonable and appropriate safeguards to protect it.

(4) Report to the Covered Entity any Security Incident of which it becomes aware. For the purposes of this BAA and the Agreement, Security Incident means, as set forth in 45 C.F.R. Section 164.304, “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 not include, (a) unsuccessful attempts to penetrate computer networks or servers maintained by Business Associate, or (b) immaterial incidents that occur on a routine basis, such as general “pinging” or “denial of service” attacks.

i. Amendment of PHI. Within ten (10) days of receipt of a request from Covered Entity for an amendment of Protected Information or a record about an individual contained in a Designated Record Set, Business Associate or its agents or subcontractors shall make such Protected Information available to Covered Entity for amendment and incorporate any such amendment to enable Covered Entity to fulfill its obligations under the Privacy Rule. If any individual requests an amendment of Protected Information directly from Business Associate or its agents or subcontractors, Business Associate must notify Covered Entity in writing within five (5) days of the request. Any approval or denial of amendment of Protected Information maintained by Business Associate or its agents or subcontractors shall be the responsibility of Covered Entity.

j. Accounting Rights. Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an individual for an accounting of disclosures of PHI in accordance with the Privacy Rule and the HITECH Act. [42 U.S.C. Section 17935(c) and 45 C.F.R. Section 164.528]. Business Associate agrees to implement a process that allows for an accounting of disclosures to be collected and maintained by Business Associate and its agents or subcontractors for at least six (6) years prior to the request. Accounting of disclosures from an Electronic Health Record for treatment, payment or health care operations purposes are required to be collected and maintained for three (3) years prior to the request, and only to the extent Business Associate maintains an electronic health record and is subject to this requirement.

At a minimum, the information collected and maintained shall include: (i) the date of disclosure; (ii) the name of the entity or person who received Protected Information and, if known, the address of the entity or person; (iii) a brief description of Protected Information disclosed and (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual’s authorization, or a copy of the written request for disclosure. [45 C.F.R. Section 164.528(b)]. In the event that the request for an accounting is delivered directly to Business Associate or its agents or subcontractors, Business Associate shall forward it to Covered Entity in writing within five (5) days of the request. It shall be Covered Entity’s responsibility to prepare and deliver any such accounting requested. Business Associate shall not disclose any Protected Information except as set forth in the Agreement and this BAA.

k. Governmental Access to Records. Business Associate shall make its internal practices, books, and records relating to the use and disclosure of Protected Information available and to the Secretary of the U.S. Department of Health and Human Services (the “Secretary”) for purposes of determining Business Associate’s compliance with the Privacy Rule

[45 C.F.R. Section 165.504(e)(2)(ii)(I). Business Associate shall concurrently provide to Covered Entity a copy of any internal practices, books, and records relating the use and disclosure of PHI that Business Associate provides to the Secretary.

I. Minimum Necessary. Business Associate and its agents or subcontractors shall request, use, and disclose only the minimum amount of Protected Information reasonably necessary to accomplish the purpose of the request, use, or disclosure in accordance with 42 U.S.C. Section 17935(b).

m. Data Ownership. Business Associate acknowledges that Business Associate has no ownership rights with respect to the Protected Information governed by this BAA, and all rights, interests, and title remain vested in the County at all times.

Business Associate shall notify Covered Entity within ten (10) days of learning that Business Associate has become the subject of an audit, compliance review, or complaint investigation by the Office for Civil Rights of the U.S. Department of Health and Human Services.

III. Termination

a. Material Breach. A Breach by Business Associate of any provision of this BAA shall constitute a material breach of the Agreement and shall provide grounds for immediate termination of the Agreement, notwithstanding any provision in the Agreement to the contrary. [45 C.F.R. Section 164.504(e)(2)(iii)].

b. Judicial or Administrative Proceedings. Covered Entity may terminate the Agreement, effective immediately, if (i) Business Associate is named as a defendant in a criminal proceeding for a violation of HIPAA, the HITECH Act, 42 C.F.R. Part 2, the HIPAA Regulations or other security or privacy laws; or (ii) a finding or stipulation that the Business Associate has violated any standard or requirement of HIPAA, the HITECH Act, 42 C.F.R. Part 2, the HIPAA Regulations or other security or privacy laws is made in any administrative or civil proceeding.

c. Effect of Termination. Upon termination of the Agreement for any reason, Business Associate shall, at the option of Covered Entity, immediately return or destroy all Protected Information that Business Associate or its agents or subcontractors still maintain in any form, and shall retain no copies of such Protected Information. If return or destruction is not feasible, Business Associate shall continue to extend the protections of Section II of the BAA to such information, and limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible. [45 C.F.R. Section 164.504(e) (ii)(2)(I)]. If County elects destruction of the PHI, Business Associate shall certify in writing to County that such PHI has been destroyed.

IV. General Provisions

a. Indemnification. In addition to the indemnification language in the Agreement, Business Associate agrees (i) to be responsible for, and defend, indemnify, and hold harmless the Covered Entity for any breach of Business Associate's privacy or security obligations under the Agreement, including any fines, penalties, and assessments that may be made against Covered Entity or the Business Associate for any Privacy Breaches or late reporting; and (ii) to pay and bear responsibility for the cost of and notice for any credit monitoring services.

b. Disclaimer. Covered Entity makes no warranty or representation that compliance by Business Associate with this BAA, HIPAA, the HITECH Act, or the HIPAA Regulations will be adequate or satisfactory for Business Associate's own purposes. Business Associate is solely responsible for all decisions made by Business Associate regarding the use and safeguarding of PHI.

c. Amendment to Comply with Law. The parties acknowledge that state and federal laws relating to data security and privacy are evolving and that amendment of the Agreement or BAA may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule and other applicable California laws relating to the security or confidentiality of PHI. Upon the request of any Party, the other Party agrees to promptly enter into negotiations concerning the terms of an amendment to the BAA embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule and other applicable California laws relating to the security or confidentiality of PHI.

Covered Entity may terminate the Agreement between the Parties or this BAA upon thirty (30) days written notice in the event (i) Business Associate does not promptly enter into negotiations to amend the Agreement when requested by Covered Entity pursuant to this section or (ii) Business Associate does not enter into an amendment to the Agreement providing assurances regarding the safeguarding of PHI that Covered Entity, in its sole discretion, deems sufficient to satisfy the standards and requirements of applicable laws.

d. Assistance in Litigation of Administrative Proceedings. Business Associate shall notify Covered Entity within forty-eight (48) hours of any litigation or administrative proceedings commenced against Business Associate or its agents or subcontractors. Business Associate shall make itself, and any subcontractors, employees, or agents assisting Business Associate in the performance of its obligations under the Agreement or BAA, available to Covered Entity, at no cost to Covered Entity, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against Covered Entity, officers or employees based upon a claimed violation of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule, or other laws relating to security and privacy, except where Business Associate or its subcontractor, employee, or agent is named as an adverse party.

e. No Third-Party Beneficiaries. Nothing express or implied in the Agreement or this BAA is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Business Associate, and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

f. Effect on Agreement. Except as specifically required to implement the purposes of the BAA, or to the extent inconsistent with this BAA, all other terms of the Agreement shall remain in force and effect.

g. Interpretation. The BAA shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, the Privacy Rule, and the Security Rule. The parties agree that any ambiguity in this BAA shall be resolved in favor of a meaning that complies and

is consistent with HIPAA, the HITECH Act, 42 C.F.R. Part 2, the Privacy Rule, and the Security Rule and other applicable California laws relating to the security or confidentiality of PHI.

h. Governing Law, Venue. This Business Associate Agreement has been executed and delivered in, and shall be construed and enforced in accordance with, the Underlying Agreement.

i. Survivorship. The respective rights and responsibilities of Business Associate related to the handling of PHI survive termination of this Agreement.

V. Drug and Alcohol Records

a. To the extent applicable, Covered Entity and Business Associate agree that when drug and alcohol treatment records are included in the contracted scope of services, the Business Associate will act as a “qualified service organization” or a “QSO” within the meaning of the federal law governing Confidentiality of Alcohol and Drug Abuse Patient Records and its implementing regulations, 42 C.F.R. Part 2; and

b. To the extent applicable, Adherence to the Requirements of 42 C.F.R. Business Associate acknowledges that in receiving, transmitting, transporting, storing, processing, or otherwise dealing with records and information for CSCHS patients under this Agreement and BAA, it is fully bound by the regulations governing confidentiality of alcohol and drug abuse patient records, 42 C.F.R. Section 2.1 *et seq.*, and HIPAA, and may not use or disclose the information except as permitted or required by this BAA or applicable law.

c. To the extent applicable, Resist Efforts in Judicial Procedures. Business Associate agrees to resist any efforts in judicial proceedings to obtain access to the Protected Information except as expressly provided for in the regulations governing the Confidentiality of Alcohol and Drug Abuse Records, 42 C.F.R. Part 2.

EXHIBIT-E
COUNTY INFORMATION TECHNOLOGY USER RESPONSIBILITY STATEMENT
FOR THIRD PARTIES

1. DEFINITIONS

- (a) “*County Confidential Information*” is all material non-public information, written or oral, disclosed, directly or indirectly, through any means of communication or observation by County to Contractor or any of its affiliates or representatives.
- (b) “*County Systems*” include but are not limited to, all County-owned, leased or managed servers, mainframe computers, desktop computers, laptop computers, handheld devices (including smart phones, wireless PDAs and Pocket PCs), equipment, networks, application systems, databases, software, phone systems, any device with network capabilities (e.g., a workstation with an attached modem, routers, switches, laptop computers, handheld devices), and any other system that stores, processes, and/or transmits County-owned information/data. These items are typically under the direct control and management of the County. “*County Systems*” also include these items when they are under the control and management of a service provider for use by County, as well as any personally-owned device that an individual has express written permission to use for County purposes.
- (c) “*County-owned information/data,*” for purposes of this Exhibit is any information or data that is transported across a County network, or that resides in a County-owned information system, or on a network or system under the control and management of a service provider for use by County. This information/data is the exclusive property of County unless constitutional provision, State or Federal statute or case law provide otherwise. County-owned information/data does not include a User’s personal, nonCounty business information, communications, data, files and/or software transmitted by or stored on a personally-owned device if that information/data is not transported across a County network or does not reside in a County System or on a network or system under the control and management of a service provider for use by County.
- (d) “*Mobile Device*” is any portable computing device that fits one of the following categories: laptops, smartphones, or tablets. “*Mobile Device*” does not include devices that are used exclusively for the purpose of making telephone calls.
- (e) “*Users*” include all employees, agents and/or representatives of Contractor performing services under this Agreement.

2. GENERAL REQUIREMENTS

- (a) Contractor will provide Customer with an electronic copy of this Exhibit and will ensure, that Users know, understand and comply with the requirements of this Exhibit. In all cases, such access shall be subject to approval by an authorized County representative.
- (b) Users are responsible for knowing and understanding these requirements, and are responsible for any actions they take that do not comply with County policies and standards. If a User is unclear as to requirements, User shall ask County for guidance.

- (c) If a User is issued an account for a County System, User shall comply with the following County standards for password definition, use, and management:
- (i) Minimum password length is 12 characters unless a particular County System has a different requirement or is not technically feasible.
 - (ii) The password must be high complexity (contains one of each, upper, lower, number, symbol).
 - (iii) The password must be rotated every 90 days.
 - (iv) User must not reuse the last 10 passwords.
 - (v) Access to County System is denied after 5 failed logon attempts.
- (d) Only authorized County staff may attach any form of computer equipment to a County network or system. This includes, but is not limited to, attachment of such devices as mobile devices, peripherals (e.g., external hard drives, printers), and USB storage media. It excludes County wireless networks provided specifically for the use of guests or visitors to County facilities.
- (e) User shall not use USB storage media on any County System. All such devices shall be County-owned, formally issued to User by County, and used only for legitimate County purposes.
- (f) User shall not connect County-owned computing equipment, including USB storage media, to non-County systems or networks, unless County gives its express written permission. This formal approval process ensures that the non-County system or network in question has been evaluated for compliance with County security standards. An example of a permitted connection to a non-County system or network would be approved connection of a County issued laptop to a home network.
- (g) User shall not install, configure, or use any device intended to provide connectivity to a non-County network or system (such as the Internet), on any County System, without County's express written permission. If authorized to install, configure or use such a device, User shall comply with all applicable County standards designed to ensure the privacy and protection of data, and the safety and security of County Systems. Any allowed installation shall not be activated until it is reviewed and approved in writing by an authorized County representative.
- (h) The unauthorized implementation or configuration of encryption, special passwords, biometric technologies, or any other methods to prevent access to County resources by those individuals who would otherwise be legitimately authorized to do so is prohibited.
- (i) Users shall not attempt to elevate or enhance their assigned level of privileges unless County gives its express written permission. Users who have been granted enhanced privileges due to their specific roles, such as system or network administrators, shall not abuse these privileges and shall use such privileges only in the performance of appropriate, services performed under this Agreement.
- (j) Users shall use County-approved authentication mechanisms when accessing County networks and systems, and shall not deactivate, disable, disrupt, or bypass (or *attempt* to deactivate, disable, disrupt, or bypass) any security measure or security configuration implemented by County.

- (k) Users shall not circumvent, or attempt to circumvent, legal guidelines on software use and licensing. If a User is unclear as to whether a software program may be legitimately copied or installed, it is the responsibility of the User to check with County.
- (l) All software on County Systems shall be installed by authorized County support staff except as provided in this Agreement. Users may not download or install software on any County system unless express written permission has been obtained from County such as in this Agreement.
- (m) Users shall immediately report to the County TechLink Center the loss or theft of County-owned computer equipment, or of personally-owned computer equipment that has been approved for use in conducting County business or performing services under a Supplemental Agreement. The County Service Desk contact information is (408) 9702222 or support@tss.sccgov.org.
- (n) Users must be aware of security issues and shall immediately report incidents to the County Information Security Office involving breaches of the security of County Systems or breaches of County-owned information/data, such as the installation of an unauthorized device, or a suspected software virus or other occurrences of malicious software or content. The Information Security Office's contact information is cybersecurityteam@iso.sccgov.org.
- (o) Users shall respect the sensitivity, privacy and confidentiality aspects of all County-owned information. In particular:
 - (i) Users shall not access, or attempt to access, County Systems or County-owned information/data unless specifically authorized to do so by the terms of this Agreement.
 - (ii) If User is assigned a County account, User shall not allow unauthorized individuals to use their account; this includes the sharing of account passwords.
 - (iii) Users shall not without County's written permission, use or disclose County-owned information/data other than in the performance of its obligations under this Agreement.
 - (iv) Users shall take every precaution to ensure that all confidential or restricted information is protected from disclosure to unauthorized individuals.
 - (v) Users shall not make or store paper or electronic copies of information unless required to provide services under this Agreement.
 - (vi) Users shall comply with all confidentiality requirements in Contractor's Agreement with the County. Users shall not use or disclose County Confidential Information other than in the performance of its obligations for County. All County Confidential Information shall remain the property of the County. User shall not acquire any ownership interest in County Confidential Information.
- (p) Users shall do all of the following:
 - (i) Users shall not change or delete County-owned information/data unless performing such changes is required to perform services under this Agreement.

- (ii) Users shall avoid actions that might introduce malicious software, such as viruses or worms, onto any County system or network.
- (iii) Upon termination or expiration of this Agreement, Users shall not retain, give away, or remove any County-owned information/data or document from any County System or County premises. Users shall return to County all County-owned assets, including hardware and data.
- (q) Electronic information transported across any County network, or residing in any County System, is potentially subject to access by County technical support staff, other County personnel, and the general public. Users should not presume any level of privacy for data transmitted over a County network or stored on a County System.
- (r) Users must protect, respect and not infringe upon all intellectual property rights, including but not limited to rights associated with patents, copyrights, trademarks, trade secrets, proprietary information, County Confidential Information, and confidential information belonging to any other third party.
- (s) All information resources on any County System are the property of County and are therefore subject to County policies regarding acceptable use. No User may use any County System or County-owned information/data for the following purposes:
 - (i) Personal profit, including commercial solicitation or conducting or pursuing their own business interests or those of another organization that are not related to the User conducting County business. This prohibition does not apply to User's performance of contractual obligations for the County.
 - (ii) Unlawful or illegal activities, including downloading licensed material without authorization, or downloading copyrighted material from the Internet without the publisher's permission.
 - (iii) To access, create, transmit, print, download or solicit material that is, or may be construed to be, harassing or demeaning toward any individual or group for any reason, including but not limited to on the basis of sex, age, race, color, national origin, creed, disability, political beliefs, organizational affiliation, or sexual orientation, unless doing so is legally permissible and necessary in the course of conducting County business.
 - (iv) To access, create, transmit, print, download or solicit sexually-oriented messages or images, or other potentially offensive materials such as, but not limited to, violence, unless doing so is legally permissible and necessary in the course of conducting County business.
 - (v) Knowingly propagating or downloading viruses or other malicious software.
 - (vi) Disseminating hoaxes, chain letters, or advertisements.

3. INTERNET AND EMAIL

- (a) Users shall not use County Systems for personal activities.

- (b) When conducting County business or performing services under this Agreement, Users shall not configure, access, use, or participate in any Internet-based communication or data exchange service unless express written permission has been given by County. Such services include, but are not limited to, file sharing (such as Dropbox, Box, Google OneDrive), Instant Messaging (such as AOL IM), email services (such as Hotmail and Gmail), peer-to-peer networking services (such as Kazaa), and social networking services (such as blogs, Instagram, Snapchat, MySpace, Facebook and Twitter). If a User has received express written permission to access such services, User shall comply with all relevant County policies, procedures, and guidelines.
- (c) Users assigned a County email account must comply with the County's Records Retention and Destruction Policy.
- (d) Users shall not use an internal County email account assigned to another individual to either send or receive email messages.
- (e) Users shall not configure a County email account so that it automatically forwards messages to an external Internet email system unless County gives its express written permission.

4. REMOTE ACCESS

- (a) Users are not permitted to implement, configure, or use any remote access mechanism unless the County has authorized the remote access mechanism.
- (b) County may monitor and/or record remote access sessions, and complete information on the session logged and archived. Users have no right, or expectation, of privacy when remotely accessing County Systems or County-owned information/data. County may use audit tools to create detailed records of all remote access attempts and remote access sessions, including User identifier, date, and time of each access attempt.
- (c) User shall configure all computer devices used to access County resources from a remote location according to NIST 800-53 standards, or an equivalent industry standard.

These include approved, installed, active, and current: anti-virus software, software or hardware-based firewall, full hard drive encryption, and any other security software or security-related system configurations that are required and approved by County.
- (d) Users that have been provided with a County-owned device intended for remote access use, such as a laptop or other Mobile Device, shall ensure that the device is protected from damage, access by third parties, loss, or theft. Users shall immediately report loss or theft of such devices to the County Service Desk: (408) 970-2222 or support@tss.sccgov.org.
- (e) Users shall protect the integrity of County Systems and County-owned information/data while remotely accessing County resources, and shall immediately report any suspected security incident or concern to the County Information Security Office at cybersecurityteam@iso.sccgov.org.
- (f) Users shall comply with any additional remote access requirements in this Agreement such as an Exhibit on Remote Access.

5. THIRD PARTY-OWNED DEVICES

- (a) This Section 5 applies if County permits Users to perform services under this Agreement with devices not owned by the County (“Third-party owned device”). Third-party owned devices include devices with email and/or data storage capability (such as laptops, iPhones, iPads, Android phones and tablets, BlackBerry and other “smart” devices).
- (b) The third party-owned device in question shall use existing, County-approved and County-owned access/authentication systems when accessing County Systems.
- (c) Users shall allow County to configure third party-owned devices as appropriate to meet security requirements, including the installation of specific security software mandated by County policy.
- (d) Use of a third party-owned device shall comply with County policies and procedures for ensuring that software updates and patches are applied to the device according to a regular, periodic schedule on at least a monthly basis. County may verify software installations and updates.
- (e) Users have no expectation of privacy with respect to any County-owned communications, information, or files on any third party-owned device. User agrees that, upon request, the County may immediately access any and all work-related or County-owned information/ data stored on these devices, in order to ensure compliance with County policies.
- (f) Users shall adhere to all relevant County security policies and standards, just as if the third party-owned device were County property. This includes, but is not limited to, policies regarding password construction and management, physical security of the device, device configuration including full storage encryption, and hard drive and/or storage sanitization prior to disposal.
- (g) Users shall not make modifications of any kind to operating system configurations implemented by County on the device for security purposes, or to any hardware or software installed on the device by County.
- (h) Users shall treat the contract-related or County-owned communications, information or files the third-party owned device contains as County property. User shall not allow access to or use of any work-related or County-owned communications, information, or files by individuals who have not been authorized by County to access or use that data.
- (i) Users shall report immediately to the County Information Security Office cybersecurityteam@iso.sccgov.org, any incident or suspected incident of unauthorized access and/or disclosure of County resources, data, or networks that involve the thirdparty owned device, and shall report the loss or theft of the device immediately to the County Service Desk: (408) 970-2222 or support@tss.sccgov.org.

6. ACKNOWLEDGEMENT AND RECEIPT

This Acknowledgement hereby incorporates the URS.

By signing below, I acknowledge that I have read and understand all sections of this URS. I also acknowledge that violation of any of its provisions may result in disciplinary action, up to and including termination of my relationship with County and/or criminal prosecution.

Have you been granted Remote Access X Yes No

I have read and understand the contents of the URS regarding Remote Access and the Exhibit on Remote Access. I understand that violation of these provisions may result in disciplinary action, up to and including termination of my relationship with the County and/or criminal prosecution. I received approval from County for remote access for legitimate County business, as evidenced by the signatures below.

User Signature:

Date Signed:

Print User Name:

Exhibit-F
REMOTE ACCESS

1. Definitions

- (a) "Remote Access" is the act of accessing County Systems from a non-County network infrastructure.
- (b) "County Systems," for purposes of this Exhibit, include but are not limited to, all County-owned, leased or managed servers, mainframe computers, desktop computers, laptop computers, handheld devices (including smart phones, wireless PDAs and Pocket PCs), equipment, networks, application systems, databases, software, phone systems, any device with network capabilities (e.g., a workstation with an attached modem, routers, switches, laptop computers, handheld devices), and any other system that stores, processes, and/or transmits County-owned information/data. These items are typically under the direct control and management of the County. "County Systems" also include these items when they are under the control and management of a service provider for use by County, as well as any personally-owned device that an individual has express written permission to use for County purposes.
- (c) "County-owned information/data," for purposes of this Exhibit, is any information or data that is transported across a County network, or that resides in a County-owned information system, or on a network or system under the control and management of a service provider for use by County. This information/data is the exclusive property of County unless constitutional provision, State or Federal statute or case law provide otherwise. County-owned information/data does not include a User's personal, non-County business information, communications, system data, files and/or software transmitted by or stored on a personally-owned device if that information/data is not transported across a County network or does not reside in a County System or on a network or system under the control and management of a service provider for use by County.
- (d) "Contractor employees" includes Contractor's employees, agents, representatives, contractors or subcontractors performing services under this Agreement.

2. Scope of Access

- (a) County grants Remote Access privileges (through the method described in section 9) for Contractor to access the following County Systems (collectively referred to as "Designated Systems"), in accordance with the terms of this Agreement:
RALS-Web3: RCS-1879
- (b) All other forms of access to the Designated Systems, or to any County System that is not specifically named, is prohibited.
- (c) Remote Access is granted for the purpose of Contractor providing services and performing its obligations as set forth in this Agreement including, but not limited to, supporting Contractor-installed programs. Any access to the Designated Systems, County-owned information/data, or any other County System or asset that is not specifically authorized under the terms of this Agreement is prohibited and is a material breach that may result in immediate termination of this Agreement for cause and any penalty allowed by law. Contractor may only access the Designated Systems

(d) County will review the scope of Contractor's Remote Access rights periodically.

3. Security Requirements

- (a) Contractor will not install any Remote Access capabilities on any County System unless such installation and configuration is approved by the County Information Security Office and meets or exceeds NIST 800-53 standards, or an equivalent industry standard.
- (b) Contractor will only remotely access Designated Systems, including access initiated from a County System, if the following conditions are met:
 - (i) Upon request by an authorized County representative, Contractor will submit documentation verifying its own network security mechanisms to County for County's review and approval. The County reserves the right to advanced written approval of Contractor's security mechanisms prior to Contractor being granted Remote Access.
 - (ii) The Remote Access method agreed upon pursuant to paragraph 9 must include the following minimum control mechanisms:
 - (aa) Two-Factor Authentication: An authentication method that requires two of the following three factors to confirm the identity of the user attempting Remote Access. Those factors include: 1) something you possess (e.g., security token and/or smart card); 2) something you know (e.g., a personal identification number (PIN)); or 3) something you are (e.g., fingerprints, retina scan). The only exceptions are County approved County-site-to-Contractor-site Virtual Private Network (VPN) infrastructure.
 - (bb) County personnel will control authorizations (permissions) to specific systems or networks.
 - (cc) All Contractor systems used to remotely access County Systems must have industry-standard anti-virus and other security measures that might be required by the County (e.g., software firewall) installed, configured, and activated.

4. Monitoring/Audit

County will monitor access to, and activities on, County Systems, including all Remote Access attempts. Data on all activities will be logged on a County System and will include the date, time, and user identification.

5. Copying, Deleting or Modifying Data

Contractor is prohibited from copying, modifying, or deleting any data contained in or on any County System unless otherwise stated in this Agreement or unless Contractor receives prior written approval from County. This does not include data installed by the Contractor to fulfill its obligations as set forth in this Agreement.

6. Connections to Non-County Networks and/or Systems

Contractor agrees to make every effort to protect data contained on County Systems within Contractor's control from unauthorized access. Prior written approval is required before Contractor may access County Systems from a non-designated system. Such access will use information security protocols that meet or exceed NIST 800-53 standards, or an equivalent industry standard. Remote Access must include the control mechanisms noted in Paragraph 3(b)(ii) above.

7. Remote Access Contacts

The following persons are points of contact for purposes of this Exhibit:

Contractor: [Wesley Reaves, Wesley.Reaves@abbott.com]

County: Stephen Wong, Clinical Lab Scientist Manager, Stephen.Wong@hhs.sccgov.org

Either party may change the aforementioned names by providing the other party with no less than three (3) business days prior written notice.

8. Additional Requirements

Contractor agrees to the following:

- (a) Only Contractor employees providing services or fulfilling Contractor obligations under this Agreement will be given Remote Access rights.
- (b) Any access to Designated Systems, other County Systems and/or County-owned information/data that is not specifically authorized under the terms of this Agreement is prohibited and is a material breach that may result in immediate termination of the Agreement for cause and any other penalty allowed by law.
- (c) An encryption method that meets or exceeds Federal Information Processing Standard (FIPS) Publication 140-2 will be used.
- (d) Contractor shall protect the integrity of County Systems and County-owned information/data while remotely accessing County resources, and shall report any suspected security incident or concern to the County Service Desk within 24 hours: (408) 970-2222 or support@tss.sccgov.org.
- (e) Contractor shall ensure compliance with the terms of this Exhibit and the Exhibit on County Information Technology User Responsibility Statement for Third Parties by all Contractor employees performing services under this Agreement.
- (f) Contractor employees have no right, or expectation, of privacy when remotely accessing County Systems or County-owned information/data. County may use audit tools to create detailed records of all remote access attempts and remote access sessions, including User identifier, date, and time of each access attempt.
- (g) Contractor employees that have been provided with a County-owned device intended for remote access use, such as a laptop or other Mobile Device, shall ensure that the device is protected from damage, access by third parties, loss, or theft. Contractor employees shall report loss or theft of such devices to the County Service Desk within 24 hours: (408) 970-2222 or support@tss.sccgov.org.

9. Remote Access Methods

- (a) All forms of Remote Access will be made in accordance with mutually agreed upon industry standard protocols and procedures, which must be approved in writing by the County. The remote access solution must conform to County policy and security requirements.
- (b) Remote Access Back-Up Method may be used in the event that the primary method of Remote Access is inoperable.
- (c) Contractor agrees to abide by the following provisions related to the Primary and (if applicable) Backup Remote Access Methods selected below. (Please mark appropriate box for each applicable Remote Access Method; if a method is not applicable, please check the button marked N/A).

(i) **VPN Site-to-Site** **Primary** **Backup** **N/A**

The VPN Site-to-Site method involves a VPN concentrator at both the Contractor site and at the County, with a secure “tunnel” opened between the two concentrators. If using the VPN Site-to-Site Method, Contractor support staff will have access to the Designated Systems from selected network-attached devices at the Contractor site.

(ii) VPN Client Access **Primary** **Backup** **N/A**

In the VPN Client Access method, a VPN Client (software) is installed on one or more specific devices at the Contractor site, with Remote Access to the County (via a County VPN concentrator) granted from those specific devices only.

An Authentication Token (a physical device or software token that an authorized remote access user is given for user authentication purposes, such as a CryptoCard, RSA token, SecureAuth IdP, Arcot software token, or other such one-time-password mechanism approved by the County Information Security Office) will be issued to the Contractor in order to authenticate Contractor staff when accessing County Designated Systems via this method. The Contractor agrees to the following when issued an Authentication Token:

- a. Because the Authentication Token allows access to privileged or confidential information residing on the County’s Designated Systems, the Contractor agrees to treat the Authentication Token as it would a signature authorizing a financial commitment on the part of the Contractor.
- b. A hardware Authentication Token is a County-owned physical device, and will be labeled as such. The label must remain attached at all times.
- c. The Authentication Token is issued to an individual employee of the Contractor and may only be used by the designated individual.
- d. The Authentication Token must be kept in the possession of the individual Contractor employee it was issued to or in a secured environment under the direct control of the Contractor, such as a locked office where public or other unauthorized access is not allowed.
- e. If the Contractor’s remote access equipment is moved to a non-secured site, such as a repair location, the Authentication Token will be kept under Contractor control.
- f. If the Authentication Token is misplaced, stolen, or damaged, the Contractor will notify the County TechLink Center by phone within 24 hours.
- g. Contractor agrees to use the Authentication Token as part of its normal business operations and for legitimate business purposes only.
- h. The Authentication Token will be issued to Contractor following execution of this Agreement. Hardware Authentication Tokens will be returned to the County’s Tech Link Center within five (5) business days following contract termination, or upon written request of the County for any reason.
- i. Contractor will notify the County’s the County TechLink Center within one working day of any change in personnel affecting use and possession of the Authentication Token. The County Service Desk contact information is (408) 970-2222 or support@tss.sccgov.org. Contractor will obtain the Authentication Token from any employee who no longer has a legitimate need to possess the Authentication Token. The County will recoup the cost of any lost or non-returned hardware Authentication.
- j. Contractor will not store account or password documentation or PINs with Authentication Tokens.

- k. Contractor will ensure all Contractor employees that are issued an Authentication Token will be made aware of and provided with a written copy of the requirements set forth in this Exhibit.

(iii) County-Controlled VPN Client Access Primary Backup N/A

This form of Remote Access is similar to VPN Client access, except that the County will maintain control of the Authentication Token and a PIN number will be provided to the Contractor for use as identification for Remote Access purposes. When the Contractor needs to access County Designated Systems, the Contractor must first notify the County's Remote Access Contact.

The County's TechLink Center will verify the PIN number provided by the Contractor. After verification of the PIN the County's designee will give the Contractor a one-time password which will be used to authenticate Contractor when accessing the County's Designated Systems. Contractor agrees to the following:

- a. Because the PIN number allows access to privileged or confidential information residing on the County's Designated Systems, the Contractor agrees to treat the PIN number as it would a signature authorizing a financial commitment on the part of the Contractor.
- b. The PIN number is confidential, County-owned, and will be identified as such.
- c. The PIN number must be kept in a secured environment under the direct control of the Contractor, such as a locked office where public or other unauthorized access is not allowed.
- d. If the Contractor's remote access equipment is moved to a non-secured site, such as a repair location, the PIN number will be kept under Contractor control.
- e. The PIN number can only be released to an authorized employee of the Contractor and may only be used by the designated individual.
- f. If the PIN number is compromised or misused, the Contractor will notify the County's designee within one (1) business day.
- g. Contractor will use the PIN number as part its normal business operations and for legitimate business purposes only. Any access to Designated Systems, other County Systems, and/or County-owned information/data that is not specifically authorized under the terms of this Agreement is prohibited and is a material breach that may result in immediate termination of the Agreement for cause and any other penalty allowed by law.
- h. The PIN number will be issued to Contractor following execution of this Agreement.
- i. The PIN number will be inactivated by the County's designee within five (5) business days following contract termination, or as required by the County for any reason.

(iv) County-Controlled Enexity Access Primary Backup N/A

The County-Controlled Enexity Access method involves using Securelink's Enexity tool installed in the County. County will establish a gateway where Contractor can access the Designated Systems from selected network-attached devices at the County site. County will control the access list for Contractors with access through Enexity gateways.

Signatures of Contractor Employees receiving Authentication Tokens (**Only for VPN Client Access and if tokens issued by County**):

SIGNATURE: _____
[TYPE NAME AND TITLE HERE.]
Date: _____

SIGNATURE: _____
[TYPE NAME AND TITLE HERE.]
Date: _____

SIGNATURE: _____
[TYPE NAME AND TITLE HERE.]
Date: _____

SIGNATURE: _____
[TYPE NAME AND TITLE HERE.]
Date: _____

EXHIBIT-G
CONTRACTOR CERTIFICATION OF COMPLIANCE WITH
COVID-19 VACCINE REQUIREMENTS
(Revised January 4, 2022)

Contractor Information:

Contractor name: _____ Name of Contractor representative: _____
Abbott Rapid Diagnostics Informatics, Inc. Mike McNamara

Contractor phone number: _____ Contractor email address: _____
480-221-3476 mike.mcnamara@abbott.com

County Department(s) where work is COVID-19 Designee for the County performed:
Department: _____

Contractor Certification. On behalf of Contractor, I hereby certify that:

1. Contractor has reviewed and is in compliance with all current County requirements regarding COVID-19 vaccination applicable to contractor’s employees working at County facilities, including but not limited to the requirements in the County’s memorandum regarding COVID19 Vaccine Requirement for County Personnel (“County Vaccine Policy”), the County’s memorandum regarding Application of COVID-19 Vaccination Requirement to County Contractors, Interns, and Volunteers, all current State and County Health Officer orders, and any other County requirements. These memoranda and current County policies are accessible at <<https://procurement.sccgov.org/doing-business-county/contractor-vaccinations>>. Contractor has also reviewed and is in compliance with the State of California’s July 26, 2021 Public Health Order and December 22, 2021 Public Health Orders. Contractor understands that it is responsible for reviewing and maintaining compliance with all subsequent revisions or amendments to State and County orders and requirements regarding COVID-19.
2. As of the date signed below:
 - a. Contractor understands that it must confirm, and has confirmed, that all of contractor’s workers (including any subcontractor workers) who routinely perform services for the County onsite and share airspace with or proximity to other people at a County facility as part of their services for the County¹ are:
 - i. Fully vaccinated against COVID-19 and, as of January 24, 2022, up-to-date on any boosters for which they are eligible as defined and required in the County Vaccine Policy; **or**

- ii. Have a legally sufficient and approved medical, disability, or religious exemption from vaccination that has been granted by contractor.
 - b. Contractor has verified and will continue to verify the vaccination status of all staff working on site at any County facility, and has obtained proof of vaccination from its staff in a form consistent with the California Department of Public Health's Vaccine Records Guidelines and Standards.
3. If contractor seeks to send any workers who are not fully vaccinated and, as of January 24, 2022, up-to-date on boosters for which they are eligible, to any County facility because the contractor has granted them an exemption, contractor shall notify the County in writing by providing a list of any such workers to the COVID-19 Designee for the department that manages the facility where the contractor personnel will be working at least 96 hours in advance of any such worker arriving onsite so that the department has sufficient time to determine whether it will approve the contractor's requests that its personnel work onsite and, if approved, can ensure that the contractor has complied with all applicable COVID-19 safety requirements for unvaccinated individuals, including, where applicable, regular testing and the use of a fit-tested N95 mask.¹ Notice must be separately provided to each department that manages a facility where contractor seeks to assign personnel to work onsite. Regardless of exemption status, personnel who are not fully vaccinated and, as of January 24, 2022, up-to-date on boosters for which they are eligible may not work in higher-risk settings at County facilities.²
4. If any of contractor's workers are noncompliant with vaccination or testing requirements, contractor will notify the County Department for which they are providing services immediately and will not permit those workers to go onsite at a County facility without express written permission from the County.

//
//

¹ As established in the County's Memorandum Regarding Application of COVID-19 Vaccination Requirement to County Contractors, Interns, and Volunteers, contractors performing work at closed construction sites are not required to comply with the County's vaccination requirements, but must comply with all applicable federal, state, and local public health laws, including but not limited to vaccination, testing, and masking requirements.

² If contractor sends workers who are not fully vaccinated and, as of January 24, 2022, up-to-date on boosters for which they are eligible, it is contractor's obligation to ensure that it has any necessary authorization under the California Confidentiality of Medical Information Act, Cal. Civ. Code §§ 56 *et. seq.*, and under any other laws to share this information with the County.

³ "Higher-Risk Settings" are those identified in the Order of the Health Officer of the County of Santa Clara Requiring Upto-Date COVID-19 Vaccination of Personnel in Higher-Risk Settings, *available at*: <https://covid19.sccgov.org/december28-2021-booster-health-order>. There are certain high-risk roles and high-risk areas that are not within higher-risk settings. Regardless of exemption status, effective no later than February 1, 2022, County personnel are not permitted to work in these high-risk roles and high-risk areas if they are not fully vaccinated and, as of January 24, 2022, up-to-date.

//
//
//

-
- Contractor will comply with all reasonable requests by the County for documentation demonstrating the contractor's compliance with this Certification.

I verify the truth and accuracy of the statements in this Certification under penalty of perjury under the laws of the State of California.

Name of authorized representative of Contractor

Title

Signature

Date

Name of authorized representative of Contractor

Title

Signature

Date

EXHIBIT- I
INSURANCE REQUIREMENTS FOR
PROFESSIONAL SERVICES CONTRACTS
(e.g. Medical, Legal, Financial services, etc.)

Insurance

Without limiting the Contractor's indemnification of the County, the Contractor shall provide and maintain at its own expense, during the term of this Agreement, or as may be further required herein, the following insurance coverages and provisions:

A. Evidence of Coverage

Prior to commencement of this Agreement and upon request, the Contractor shall provide a Certificate of Insurance certifying that coverage as required herein has been obtained. Individual endorsements required herein shall accompany the certificate.

This verification of coverage shall be sent to the requesting County department, unless otherwise directed. The Contractor shall not receive a Notice to Proceed with the work under the Agreement until it has obtained all insurance required and such insurance has been approved by the County. This approval of insurance shall neither relieve nor decrease the liability of the Contractor.

B. Qualifying Insurers

All coverages, except surety, shall be issued by companies which hold a current policy holder's alphabetic and financial size category rating of not less than A- V, according to the current Best's Key Rating Guide or a company of equal financial stability that is approved by the County's Insurance Manager.

C. Notice of Cancellation

All coverage as required herein shall not be canceled or changed so as to no longer meet the specified County insurance requirements without 30 days' prior written notice of such cancellation or change being delivered to the County of Santa Clara or their designated agent.

D. Insurance Required

1. Commercial General Liability Insurance - for bodily injury (including death) and property damage which provides limits as follows:

- a. Each occurrence - \$1,000,000
- b. General aggregate - \$2,000,000
- c. Personal Injury - \$1,000,000

2. General liability coverage shall include:

- a. Premises and Operations

- b. Personal Injury liability
 - c. Severability of interest
3. General liability coverage shall include the following endorsement, a copy of which shall be provided to the County:

Additional Insured Endorsement, which shall include:

“County of Santa Clara, and members of the Board of Supervisors of the County of Santa Clara, and the officers, agents, and employees of the County of Santa Clara, individually and collectively, as additional insureds. A blanket additional insured endorsement will be acceptable.”

Insurance afforded by the additional insured endorsement shall apply as primary insurance, and other insurance maintained by the County of Santa Clara, its officers, agents, and employees shall be excess only and not contributing with insurance provided under this policy. Public Entities may also be added to the additional insured endorsement as applicable and the contractor shall be notified by the contracting department of these requirements.

4. Automobile Liability Insurance

For bodily injury (including death) and property damage which provides total limits of not less than one million dollars (\$1,000,000) combined single limit per occurrence applicable to owned, non-owned and hired vehicles.

5. Workers' Compensation and Employer's Liability Insurance

- a. Statutory California Workers' Compensation coverage including broad form all-states coverage.
- b. Employer's Liability coverage for not less than one million dollars (\$1,000,000) per occurrence.

6. Professional Errors and Omissions Liability Insurance

- a. Coverage shall be in an amount of not less than one million dollars (\$1,000,000) per claim or occurrence/aggregate.
- b. If coverage contains a deductible or self-retention, it shall not be greater than fifty thousand dollars (\$50,000) per occurrence/event.
- c. Coverage as required herein shall be maintained for a minimum of two years following termination or completion of this Agreement.

7. Claims Made Coverage

If coverage is written on a claims made basis, the Certificate of Insurance shall clearly state so. In addition to coverage requirements above, such policy shall provide that:

- a. Policy retroactive date coincides with or precedes the Contractor's start of work (including subsequent policies purchased as renewals or replacements).
- b. Policy shall be continued for five (5) years after the termination of this Agreement.

E. Special Provisions

The following provisions shall apply to this Agreement:

1. The foregoing requirements as to the types and limits of insurance coverage to be maintained by the Contractor and any approval of said insurance by the County or its insurance consultant(s) are not intended to and shall not in any manner limit or qualify the liabilities and obligations otherwise assumed by the Contractor pursuant to this Agreement, including but not limited to the provisions concerning indemnification.
2. The County acknowledges that some insurance requirements contained in this Agreement may be fulfilled by self-insurance on the part of the Contractor. However, this shall not in any way limit liabilities assumed by the Contractor under this Agreement. Any self-insurance shall be approved in writing by the County upon satisfactory evidence of financial capacity. Contractor's obligation hereunder may be satisfied in whole or in part by adequately funded self-insurance programs or self-insurance retentions.
3. Should any of the work under this Agreement be sublet, the Contractor shall require each of its subcontractors of any tier to carry the aforementioned coverages, or Contractor may insure subcontractors under its own policies.
4. The County reserves the right to withhold payments to the Contractor in the event of material noncompliance with the insurance requirements outlined above.

F. Fidelity Bonds (Required only if contractor will be receiving advanced funds or payments)

Before receiving compensation under this Agreement, Contractor will furnish County with evidence that all officials, employees, and agents handling or having access to funds received or disbursed under this Agreement, or authorized to sign or countersign checks, are covered by a BLANKET FIDELITY BOND in an amount of AT LEAST fifteen percent (15%) of the maximum financial obligation of the County cited herein. If such bond is canceled or reduced, Contractor will notify County immediately, and County may withhold further payment to Contractor until proper coverage has been obtained. Failure to give such notice may be cause for termination of this Agreement, at the option of County.