

Agreement No. 2455613C00455

AGREEMENT BETWEEN THE COUNTY OF SAN MATEO AND DOXIMITY, INC

This Agreement is entered into this Tuesday, May 6, 2025 by and between the County of San Mateo, a political subdivision of the state of California, hereinafter called "County," and Doximity, Inc, hereinafter called "Contractor."

* * *

Whereas, pursuant to Section 31000 of the California Government Code, County may contract with independent contractors for the furnishing of such services to or for County or any Department thereof; and

Whereas, it is necessary and desirable that Contractor be retained for the purpose of providing an enterprise on-call scheduling application and a telehealth platform that is HIPAA-compliant.

Now, therefore, it is agreed by the parties to this Agreement as follows:

1. Exhibits and Attachments

The following exhibits and attachments are attached to this Agreement and incorporated into this Agreement by this reference:

Exhibit A—Services

Exhibit B—Payments and Rates

Exhibit C—Service Level Agreement

2. Services to be performed by Contractor

In consideration of the payments set forth in this Agreement and in Exhibit B, Contractor shall perform services for County in accordance with the terms, conditions, and specifications set forth in this Agreement and in Exhibit A.

3. Payments

In consideration of the services provided by Contractor in accordance with all terms, conditions, and specifications set forth in this Agreement and in Exhibit A, County shall make payment to Contractor based on the rates and in the manner specified in Exhibit B. In no event shall County's total fiscal obligation under this Agreement exceed **SIX HUNDRED SEVENTY-FIVE THOUSAND DOLLARS (\$675,000)**. In the event that the County makes any advance payments, Contractor agrees to refund any amounts in excess of the amount owed by the County at the time of contract termination or expiration. Contractor is not entitled to payment for work not performed as required by this agreement.

All invoices must be approved by the Health CIO or their designee. Invoices must be sent to: HS_HIT_AccountsPayable@smcgov.org. Processing time may be delayed if invoices are not submitted electronically. Invoices are processed and paid within 45 days after the invoice date. All amounts must be paid in U.S. Dollars.

4. Term

Subject to compliance with all terms and conditions, the term of this Agreement shall be from **May 6, 2025**, through **May 5, 2030**.

5. Termination

This Agreement may be terminated by Contractor or by the Director or his/her designee at any time without a requirement of good cause upon thirty (30) days' advance written notice to the other party. Contractor shall be entitled to receive payment for work/services provided prior to termination of the Agreement.

County may terminate this Agreement or a portion of the services referenced in the Attachments and Exhibits based upon the unavailability of Federal, State, or County funds by providing written notice to Contractor as soon as is reasonably possible after County learns of said unavailability of outside funding.

County may terminate this Agreement for cause. In order to terminate for cause, County must first give Contractor notice of the alleged material breach. Contractor shall have five business days after receipt of such notice to respond and a total of ten calendar days after receipt of such notice to cure the alleged material breach. If Contractor fails to cure the breach within this period, County may immediately terminate this Agreement without further action. The option available in this paragraph is separate from the ability to terminate without cause with appropriate notice described above. In the event that County provides notice of an alleged material breach pursuant to this section, County may, in extreme circumstances, immediately suspend performance of services and payment under this Agreement if such material breach is impossible to cure, pending the resolution of the process described in this paragraph. County has sole discretion to determine what constitutes an extreme circumstance for purposes of this paragraph, and County shall use reasonable judgment in making that determination.

6. Contract Materials

At the end of this Agreement, or in the event of termination, all finished or unfinished documents, data, studies, maps, photographs, reports, and other written materials (collectively referred to as "contract materials") prepared by Contractor under this Agreement shall become the property of County and shall be promptly delivered to County. Upon termination, Contractor may make and retain a copy of such contract materials if permitted by law.

7. Relationship to Parties

Contractor agrees and understands that the work/services performed under this Agreement are performed as an independent contractor and not as an employee of County and that neither Contractor nor its employees acquire any of the rights, privileges, powers, or advantages of County employees.

8. Hold Harmless

a) General Hold Harmless

Subject to the Limitation of Liability set forth in this Agreement, both parties shall indemnify and save harmless the other party and its officers, agents, employees, and servants from all claims,

suits, or actions of every name, kind, and description resulting from this Agreement, the performance of any work or services required of the parties under this Agreement, or payments made pursuant to this Agreement brought for, or on account of, any of the following:

(A) injuries to or death of any person, including Contractor or its employees/officers/agents;

(B) damage to any property of any kind whatsoever and to whomsoever belonging;

(C) any sanctions, penalties, or claims of damages resulting from either party's failure to comply, if applicable, with the requirements set forth in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and all Federal regulations promulgated thereunder, as amended; or

(D) any other loss or cost, including but not limited to that caused by the concurrent active or passive negligence of County and/or its officers, agents, employees, or servants. However, Contractor's duty to indemnify and save harmless under this Section shall not apply to injuries or damage for which County has been found in a court of competent jurisdiction to be solely liable by reason of its own negligence or willful misconduct.

The duty of the parties to indemnify and save harmless as set forth by this Section shall include the duty to defend as set forth in Section 2778 of the California Civil Code.

b) Intellectual Property Indemnification

Contractor hereby certifies that it owns, controls, and/or licenses and retains all right, title, and/or interest in and to any intellectual property it uses in relation to this Agreement, including the design, look, feel, features, source code, content, and/or other technology relating to any part of the services it provides under this Agreement and including all related patents, inventions, trademarks, and copyrights, all applications therefore, and all trade names, service marks, know how, and trade secrets (collectively referred to as "IP Rights") except as otherwise noted by this Agreement.

Contractor warrants that the services it provides under this Agreement do not infringe, violate, trespass, or constitute the unauthorized use or misappropriation of any IP Rights of any third party. Contractor shall defend, indemnify, and hold harmless County from and against all liabilities, costs, damages, losses, and expenses (including reasonable attorney fees) arising out of or related to any claim by a third party that the services provided under this Agreement infringe or violate any third-party's IP Rights provided any such right is enforceable in the United States. Contractor's duty to defend, indemnify, and hold harmless under this Section applies only provided that: (a) County notifies Contractor promptly in writing of any notice of any such third-party claim; (b) County cooperates with Contractor in all reasonable respects in connection with the investigation and defense of any such third-party claim; (c) Contractor retains sole control of the defense of any action on any such claim and all negotiations for its settlement or compromise (provided Contractor shall not have the right to settle any criminal action, suit, or proceeding without County's prior written consent, not to be unreasonably withheld, and provided further that any settlement permitted under this Section shall not impose any financial or other obligation on County, impair any right of County, or contain any stipulation, admission, or acknowledgement of wrongdoing on the part of County without County's prior written consent, not to be unreasonably withheld); and (d) should services under this Agreement become, or in Contractor's opinion be likely to become, the subject of such a claim, or in the

event such a third party claim or threatened claim causes County's reasonable use of the services under this Agreement to be seriously endangered or disrupted, Contractor shall, at Contractor's option and expense, either: (i) procure for County the right to continue using the services without infringement or (ii) replace or modify the services so that they become non-infringing but remain functionally equivalent.

Notwithstanding anything in this Section to the contrary, Contractor will have no obligation or liability to County under this Section to the extent any otherwise covered claim is based upon: (a) any aspects of the services under this Agreement which have been modified by or for County (other than modification performed by, or at the direction of, Contractor) in such a way as to cause the alleged infringement at issue; and/or (b) any aspects of the services under this Agreement which have been used by County in a manner prohibited by this Agreement.

The duty of Contractor to indemnify and save harmless as set forth by this Section shall include the duty to defend as set forth in Section 2778 of the California Civil Code.

9. Limitation of Liability

IN NO EVENT WILL EITHER PARTY, ITS AFFILIATES, EMPLOYEES, SUBCONTRACTORS OR AGENTS HAVE ANY LIABILITY ARISING OUT OF OR RELATING TO THE AGREEMENT OR THE SERVICE FOR ANY LOSS OF BUSINESS, PROFITS, SAVINGS, GOODWILL, BUSINESS INTERRUPTION OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL (EXCEPT FOR DATA LOSS OR BREACH), COVER OR PUNITIVE DAMAGES. IN NO EVENT WILL THE AGGREGATE LIABILITY OF CONTRACTOR FOR CLAIMS ARISING OUT OF OR RELATING TO THE AGREEMENT AND THE SERVICE EXCEED TEN MILLION DOLLARS (\$10,000,000.00). EXCEPT TO THE EXTENT PROHIBITED BY APPLICABLE LAW, THE FOREGOING EXCLUSIONS AND LIMITATIONS APPLY WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY, EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR IF A PARTY'S REMEDY FAILS OF ITS ESSENTIAL PURPOSE. NO CLAIM MAY BE BROUGHT BY COUNTY MORE THAN ONE (1) YEAR AFTER ACCRUAL.

10. Assignability and Subcontracting

Contractor shall not assign this Agreement or any portion of it to a third party under this Agreement without the prior written consent of County. Any such assignment without County's prior written consent shall give County the right to automatically and immediately terminate this Agreement without penalty or advance notice.

11. Insurance

11.1. General Requirements

Contractor shall not commence work or be required to commence work under this Agreement unless and until all insurance required under this Section has been obtained and such insurance has been approved by County's Risk Management, and Contractor shall use diligence to obtain such insurance and to obtain such approval. Contractor shall furnish County with certificates of insurance evidencing the required coverage, and there shall be a specific contractual liability endorsement extending Contractor's coverage to include the contractual liability assumed by Contractor pursuant to this Agreement. These certificates shall specify or be endorsed to

provide that thirty (30) days' notice must be given, in writing, to County of any pending change in the limits of liability or of any cancellation or modification of the policy.

11.2. Workers' Compensation and Employer's Liability Insurance

Contractor shall have in effect during the entire term of this Agreement workers' compensation and employer's liability insurance providing full statutory coverage. In signing this Agreement, Contractor certifies, as required by Section 1861 of the California Labor Code, that (a) it is aware of the provisions of Section 3700 of the California Labor Code, which require every employer to be insured against liability for workers' compensation or to undertake self-insurance in accordance with the provisions of the Labor Code, and (b) it will comply with such provisions before commencing the performance of work under this Agreement.

11.3. Liability Insurance

Contractor shall take out and maintain during the term of this Agreement such bodily injury liability and property damage liability insurance as shall protect Contractor and all of its employees/officers/agents while performing work covered by this Agreement from any and all claims for damages for bodily injury, including accidental death, as well as any and all claims for property damage which may arise from Contractor's operations under this Agreement, whether such operations be by Contractor, any subcontractor, anyone directly or indirectly employed by either of them, or an agent of either of them. Such insurance shall be combined single limit bodily injury and property damage for each occurrence and shall not be less than the amounts specified below:

- (a) Comprehensive General Liability..... \$1,000,000
- (b) Professional Liability..... \$1,000,000

County and its officers, agents, employees, and servants shall be included as additional insured on such policies of insurance, which shall also contain a provision that (a) the insurance afforded thereby to County and its officers, agents, employees, and servants shall be primary insurance to the full limits of liability of the Comprehensive General Liability and Commercial Automobile Liability policies and (b) if the County or its officers, agents, employees, and servants have other insurance against the loss covered by such a policy, such other insurance shall be excess insurance only.

In the event of the breach of any provision of this Section, or in the event any notice is received which indicates any required insurance coverage will be diminished or canceled, County, at its option, may, notwithstanding any other provision of this Agreement to the contrary, immediately declare a material breach of this Agreement and suspend all further work and payment pursuant to this Agreement.

11.4. Special Insurance Requirements - Cyber Liability

Cyber Liability	<p>\$5,000,000 per claim/aggregate for Privacy and Network Security,</p> <p>\$1,000,000 per claim/aggregate for Technology Errors and Omissions</p> <p>To be carried at all times during the term of the Contract and for three years thereafter.</p>
-----------------	---

If the work involves services or goods related to computers, networks, systems, storage, or access to County data or to any data that may, alone or in combination with other data, become Confidential Information or Personally Identifiable Information, the following insurance is required.

(1) Privacy and Network Security

During the term of the Contract and for three years thereafter, maintain coverage for liability and remediation arising out of unauthorized use of or access to County data or software within Contractor's network or control. Provide coverage for liability claims, computer theft, extortion, network breach, service denial, introduction of malicious code, loss of Confidential Information, or any unintentional act, error, or omission made by users of Contractor's electronic data or systems while providing services to the County. The insurance policy must include coverage for regulatory and PCI fines and penalties, crisis management expenses, and business interruption. No exclusion/restriction for unencrypted portable devices/media may be on the policy.

(2) Technology Errors and Omissions

During the term of the Contract and for three years thereafter, maintain coverage for liabilities arising from errors, omissions, or negligent acts in rendering or failing to render computer or information technology services and technology products, including at a minimum, coverage for systems analysis, design, development, integration, modification, maintenance, repair, management, or outsourcing any of the foregoing.

12. County Responsibilities

County is solely responsible for Authorized Users' use of the Service including, without limitation (a) all communications and other information transmitted by Authorized Users to or through the Service including the quality, accuracy, legality, and appropriateness of such information; (b) Authorized Users' compliance with applicable law in connection with their use of the Service; (c) all information and results obtained from, and all conclusions, decisions, and actions based on, use of the Service; and (d) ensuring that Authorized Users use the Service to communicate with patients of County only. Contractor may suspend an Authorized User's access to the Service without liability if Contractor believes such Authorized User is using the Service in violation of the Agreement or the Terms of Service. Any breach of the Agreement by an Authorized User will be deemed a breach of the Agreement by County. County will notify Contractor immediately upon any Authorized User no longer being a part of County's workforce. Authorized User shall mean all healthcare provider members of County's workforce.

13. Compliance With Laws

All services to be performed by Contractor pursuant to this Agreement shall be performed in accordance with all applicable Federal, State, County, and municipal laws, ordinances, regulations, and executive orders, including but not limited to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Federal Regulations promulgated thereunder, as amended (if applicable), the Business Associate requirements set forth in Attachment H (if attached), the Americans with Disabilities Act of 1990, as amended, and Section 504 of the Rehabilitation Act of 1973, which prohibits discrimination on the basis of disability in programs and activities receiving any Federal or County financial assistance, as well as any required economic or other sanctions imposed by the United States government or under state law in effect during the term of the Agreement. Such services shall also be performed in accordance with all applicable ordinances and regulations, including but not limited to appropriate licensure, certification regulations, provisions pertaining to confidentiality of records, and applicable quality assurance regulations. In the event of a conflict between the terms of this Agreement and any applicable State, Federal, County, or municipal law, regulation, or executive order, the requirements of the applicable law, regulation, or executive order will take precedence over the requirements set forth in this Agreement.

Contractor will timely and accurately complete, sign, and submit all necessary documentation of compliance.

14. Non-Discrimination and Other Requirements

14.1. General Non-discrimination

No person shall be denied any services provided pursuant to this Agreement (except as limited by the scope of services) on the grounds of race, color, national origin, ancestry, age, disability (physical or mental), sex, sexual orientation, gender identity, marital or domestic partner status, religion, political beliefs or affiliation, familial or parental status (including pregnancy), medical condition (cancer-related), military service, or genetic information.

14.2. Equal Employment Opportunity

Contractor shall ensure equal employment opportunity based on objective standards of recruitment, classification, selection, promotion, compensation, performance evaluation, and management relations for all employees under this Agreement. Contractor's equal employment policies shall be made available to County upon request.

14.3. Section 504 of the Rehabilitation Act of 1973

Contractor shall comply with Section 504 of the Rehabilitation Act of 1973, as amended, which provides that no otherwise qualified individual with a disability shall, solely by reason of a disability, be excluded from the participation in, be denied the benefits of, or be subjected to discrimination in the performance of any services this Agreement. This Section applies only to contractors who are providing services to members of the public under this Agreement.

14.4. Compliance with County's Equal Benefits Ordinance

Contractor shall comply with all laws relating to the provision of benefits to its employees and their spouses or domestic partners, including, but not limited to, such laws prohibiting

discrimination in the provision of such benefits on the basis that the spouse or domestic partner of the Contractor's employee is of the same or opposite sex as the employee.

14.5. Discrimination Against Individuals with Disabilities

The nondiscrimination requirements of 41 C.F.R. 60-741.5(a) are incorporated into this Agreement as if fully set forth here, and Contractor and any subcontractor shall abide by the requirements of 41 C.F.R. 60-741.5(a). This regulation prohibits discrimination against qualified individuals on the basis of disability and requires affirmative action by covered prime contractors and subcontractors to employ and advance in employment qualified individuals with disabilities.

14.6. History of Discrimination

Contractor certifies that no finding of discrimination has been issued in the past 365 days against Contractor by the Equal Employment Opportunity Commission, the California Department of Fair Employment and Housing, or any other investigative entity. If any finding(s) of discrimination have been issued against Contractor within the past 365 days by the Equal Employment Opportunity Commission, the California Department of Fair Employment and Housing, or other investigative entity, Contractor shall provide County with a written explanation of the outcome(s) or remedy for the discrimination prior to execution of this Agreement. Failure to comply with this Section shall constitute a material breach of this Agreement and subjects the Agreement to immediate termination at the sole option of the County.

14.7. Reporting; Violation of Non-discrimination Provisions

Contractor shall report to the County Executive Officer the filing in any court or with any administrative agency of any complaint or allegation of discrimination on any of the bases prohibited by this Section of the Agreement or the Section titled "Compliance with Laws". Such duty shall include reporting of the filing of any and all charges with the Equal Employment Opportunity Commission, the California Department of Fair Employment and Housing, or any other entity charged with the investigation or adjudication of allegations covered by this subsection within 30 days of such filing, provided that within such 30 days such entity has not notified Contractor that such charges are dismissed or otherwise unfounded. Such notification shall include a general description of the circumstances involved and a general description of the kind of discrimination alleged (for example, gender-, sexual orientation-, religion-, or race-based discrimination).

Violation of the non-discrimination provisions of this Agreement shall be considered a breach of this Agreement and subject the Contractor to penalties, to be determined by the County Executive Officer, including but not limited to the following:

- i. termination of this Agreement;
- ii. disqualification of the Contractor from being considered for or being awarded a County contract for a period of up to 3 years;
- iii. liquidated damages of \$2,500 per violation; and/or
- iv. imposition of other appropriate contractual and civil remedies and sanctions, as determined by the County Executive Officer.

To effectuate the provisions of this Section, the County Executive Officer shall have the authority to offset all or any portion of the amount described in this Section against amounts due to Contractor under this Agreement or any other agreement between Contractor and County.

14.8. Compliance with Living Wage Ordinance

As required by Chapter 2.88 of the San Mateo County Ordinance Code, Contractor certifies all contractor(s) and subcontractor(s) obligated under this contract shall fully comply with the provisions of the County of San Mateo Living Wage Ordinance, including, but not limited to, paying all Covered Employees the current Living Wage and providing notice to all Covered Employees and Subcontractors as required under the Ordinance.

15. Compliance with County Employee Jury Service Ordinance

If applicable, Contractor shall comply with Chapter 2.85 of the County's Ordinance Code, which states that Contractor shall have and adhere to a written policy providing that its employees, to the extent they are full-time employees and live in San Mateo County, shall receive from the Contractor, on an annual basis, no fewer than five days of regular pay for jury service in San Mateo County, with jury pay being provided only for each day of actual jury service. The policy may provide that such employees deposit any fees received for such jury service with Contractor or that the Contractor may deduct from an employee's regular pay the fees received for jury service in San Mateo County. By signing this Agreement, Contractor certifies that it has and adheres to a policy consistent with Chapter 2.85. For purposes of this Section, if Contractor has no employees in San Mateo County, it is sufficient for Contractor to provide the following written statement to County: "For purposes of San Mateo County's jury service ordinance, Contractor certifies that it has no full-time employees who live in San Mateo County. To the extent that it hires any such employees during the term of its Agreement with San Mateo County, Contractor shall adopt a policy that complies with Chapter 2.85 of the County's Ordinance Code." The requirements of Chapter 2.85 do not apply unless this Agreement's total value listed in the Section titled "Payments", exceeds two-hundred thousand dollars (\$200,000); Contractor acknowledges that Chapter 2.85's requirements will apply if this Agreement is amended such that its total value exceeds that threshold amount.

16. Retention of Records; Right to Monitor and Audit

(a) Contractor shall maintain all required records relating to services provided under this Agreement for three (3) years after County makes final payment and all other pending matters are closed, and Contractor shall be subject to the examination and/or audit by County, a Federal grantor agency, and the State of California.

(b) Contractor shall comply with all program and fiscal reporting requirements set forth by applicable Federal, State, and local agencies and as required by County.

(c) Contractor agrees upon reasonable notice to provide to County, to any Federal or State department having monitoring or review authority, to County's authorized representative, and/or to any of their respective audit agencies access to and the right to examine all records and documents necessary to determine compliance with relevant Federal, State, and local statutes, rules, and regulations, to determine compliance with this Agreement, and to evaluate the quality, appropriateness, and timeliness of services performed.

17. Access and Retention of Books and Records

Upon written request of the Secretary of Health and Human Services, the Comptroller General, or any of their duly authorized representatives, Contractor shall make available its contracts, books, documents, and records necessary to verify the nature and extent of costs of providing Services under this Agreement. Such inspection shall be available for up to four (4) years after the rendering of such Services. This section is included pursuant to and is governed by the Social Security Act's requirements pertaining to "reasonable costs" set forth in 42 U.S.C. Section 1395x(v)(1)(I) and related regulations. No attorney-client, accountant-client, or other legal privilege will be deemed to have been waived by County, Contractor, or any Contractor's representative by virtue of this Agreement. To the extent the contracts, books, documents, and records necessary to verify the nature and extent of costs of providing Services to County require the inspection of detail records regarding faxes sent and/or received, County agrees that it will download and maintain such detail records during the required inspection period. Contractor will make those records available to County for download for 90 days from the date of the fax transmission.

18. Merger Clause; Amendments

This Agreement, including the Exhibits and Attachments attached to this Agreement and incorporated by reference, constitutes the sole Agreement of the parties to this Agreement and correctly states the rights, duties, and obligations of each party as of this document's date. In the event that any term, condition, provision, requirement, or specification set forth in the body of this Agreement conflicts with or is inconsistent with any term, condition, provision, requirement, or specification in any Exhibit and/or Attachment to this Agreement, the provisions of the body of the Agreement shall prevail. Any prior agreement, promises, negotiations, or representations between the parties not expressly stated in this document are not binding. All subsequent modifications or amendments shall be in writing and signed by the parties.

19. Controlling Law; Venue

The validity of this Agreement and of its terms, the rights and duties of the parties under this Agreement, the interpretation of this Agreement, the performance of this Agreement, and any other dispute of any nature arising out of this Agreement shall be governed by the laws of the State of California without regard to its choice of law or conflict of law rules. Any dispute arising out of this Agreement shall be venued either in the San Mateo County Superior Court or in the United States District Court for the Northern District of California.

20. Notices

Any notice, request, demand, or other communication required or permitted under this Agreement shall be deemed to be properly given when both: (1) transmitted via email to the email address listed below; and (2) sent to the physical address listed below by either being deposited in the United States mail, postage prepaid, or deposited for overnight delivery, charges prepaid, with an established overnight courier that provides a tracking number showing confirmation of receipt.

In the case of County, to:

Name/Title: Thomas Collins/Director, Portfolio and Program Management
Address: 801 Gateway Blvd, South San Francisco, CA, 94080
Telephone: (628) 258-3275
Email: tcollins@smcgov.org

Name/Title: Natalie Del Sarto/Contract Administrator
Address: 801 Gateway Blvd, South San Francisco, CA, 94080
Telephone: (650) 502-2976
Email: ndelsarto@smcgov.org

Contract Questions: HS_HIT_Contract_Management@smcgov.org
Invoice Questions: HS_HIT_AccountsPayable@smcgov.org

With a Copy to:

Name/Title: County Attorney's Office
Address: 400 County Center, 6th Floor, Redwood City, CA 94063
Telephone: (650)363-4034

In the case of Contractor, to:

Name/Title: Jennifer Chaloemtiarana, General Counsel
Address: 500 3rd Street Suite 510, San Francisco, CA 94107
Telephone: (650) 546-7775.
Email: legal@doximity.com

21. Electronic Signature

Both County and Contractor wish to permit this Agreement and future documents relating to this Agreement to be digitally signed in accordance with California law and County's Electronic Signature Administrative Memo. Any party to this Agreement may revoke such agreement to permit electronic signatures at any time in relation to all future documents by providing notice pursuant to this Agreement.

22. Reimbursable Travel Expenses

To the extent that this Agreement authorizes reimbursements to Contractor for travel, lodging, and other related expenses as defined in this section, the Contractor must comply with all the terms of this section in order to be reimbursed for travel.

- A. Estimated travel expenses must be submitted to authorized County personnel for advanced written authorization before such expenses are incurred. Significant differences between estimated and actual travel expenses may be grounds for denial of full reimbursement of actual travel expenses.

Travel Expense must be invoices separately from normal services and include the approved written Travel Authorized for expenses invoiced.

- B. Itemized receipts (copies accepted) for all reimbursable travel expenses are required to be provided as supporting documentation with all invoices submitted to the County.
- C. Unless otherwise specified in this section, the County will reimburse Contractor for reimbursable travel expenses for days when services were provided to the County. Contractor must substantiate in writing to the County the actual services rendered and the specific dates. The County will reimburse for travel at 75% of the maximum reimbursement amount for the actual costs of meals and incidental expenses on the day preceding and/or the day following days when services were provided to the County, provided that such reimbursement is reasonable, in light of travel time and other relevant factors, and is approved in writing by authorized County personnel.
- D. Unless otherwise specified within the contract, reimbursable travel expenses shall not include Local Travel. "Local Travel" means travel entirely within a fifty-mile radius of the Contractor's office and travel entirely within a fifty-mile radius of San Mateo County. Any mileage reimbursements for a Contractor's use of a personal car for reimbursable travel shall be reimbursed based on the Federal mileage reimbursement rate.
- E. The maximum reimbursement amount for the actual lodging, meal and incidental expenses is limited to the then-current Continental United States ("CONUS") rate for the location of the work being done (i.e., Redwood City for work done in Redwood City, San Mateo for work done at San Mateo Medical Center) as set forth in the Code of Federal Regulations and as listed by the website of the U.S. General Services Administration (available online at <http://www.gsa.gov/portal/content/104877> or by searching www.gsa.gov for the term 'CONUS'). County policy limits the reimbursement of lodging in designated high cost of living metropolitan areas to a maximum of double the then-current CONUS rate; for work being done outside of a designated high cost of living metropolitan area, the maximum reimbursement amount for lodging is the then-current CONUS rate.

Meal reimbursement amount is limited to separate amounts for each meal expenses (Breakfast, Lunch, and Dinner) plus an incidental amount. The County does not use the standard "per diem reimbursement" for meals by the day.
- F. The maximum reimbursement amount for the actual cost of airfare shall be limited to fares for Economy Class or below. Air travel fares will not be reimbursed for first class, business class, "economy-plus," or other such classes. Reimbursable car rental rates are restricted to the mid-level size range or below (i.e. standard size, intermediate, compact, or subcompact); costs for specialty, luxury, premium, SUV, or similar category vehicles are not reimbursable. Reimbursable ride-shares are restricted to standard or basic size vehicles (i.e., non-premium vehicles unless it results in a cost-saving to the County). Exceptions may be allowed under certain circumstances, such as unavailability of the foregoing options, with written approval from authorized County personnel. Other related travel expenses such as taxi fares, ride-shares, parking costs, train or subway costs, etc. shall be reimbursable on an actual-cost basis. Reimbursement of tips for taxi fare, or ride-share are limited to no more than 15% of the fare amount.
- G. Travel-related expenses are limited to: airfare, lodging, car rental, taxi/ride-share plus tips, tolls, incidentals (e.g. porters, baggage carriers or hotel staff), breakfast, lunch, dinner, mileage reimbursement based on Federal reimbursement rate. The County will not reimburse for alcohol.

- H. Reimbursement of tips are limited to no more than 15 percent. Non-reimbursement items (i.e., alcohol) shall be excluded when calculating the amount of the tip that is reimbursable.

23. Change Management

Either party may request a modification to this Agreement by submitting a written Change Request for review and approval. All changes, including amendments to terms, scope of services, or financial obligations, must be documented in writing through an official Amendment. Verbal or informal modifications are not valid or enforceable.

A Change Request must clearly outline the proposed modification, the reason for the change, and any potential impact. The receiving party shall review the request in good faith and respond within a reasonable timeframe.

If specified in the Board Resolution for this Agreement, the Chief of San Mateo County Health, or their designee, is authorized to approve contract amendments that adjust the County's maximum fiscal obligation by up to \$25,000 in aggregate and/or modify the contract term or scope of services, provided such changes remain within the current or revised fiscal provisions. Change requests above the authorized limit will require a Board Amendment.

Upon mutual agreement, approved modifications shall be formalized in writing, signed by authorized representatives, and incorporated into this Agreement. Unless expressly modified, all other terms and conditions shall remain in effect.

24. Cloud Computing Policy 2020

24.1. Overview

Cloud computing is defined as on-demand delivery of information technology (IT) resources through the Internet. Such services use a pool of shared resources to achieve economies of scale, provide greater flexibility, and support communication, collaboration, scheduling, sharing, and storage. In most cases, these services are provided on a contractual basis by a third-party vendor and essentially becomes an extension of the County's network. Security concerns in cloud computing include, but are not limited to:

- Loss of control over the maintenance and protection of the data
- Potential loss of privacy due to aggregation of data from other cloud consumers
- Reliance on vendor's services for the security of County data

24.2. Policy Purpose

The purpose of the Cloud Computing Policy is to safeguard the County's data and to mitigate any risks associated with utilizing cloud solutions. This policy outlines best practices to ensure that data will be properly stored and shared when using cloud computing services.

24.3. Scope

The scope of this policy includes all users of the County of San Mateo's network who uses cloud computing services, including vendors, contractors, volunteers, temporary staff, consultants, collectively known as Workforce Members, and any other party who provides services or works on the computer and/or network systems.

24.4. Policy

All cloud computing services shall undergo a security assessment, performed at the time of contract, including but not limited to: security controls, identity and authentication management, password management, auditing, and encryption capabilities. As part of the review process, all cloud services that are currently listed in the Federal Risk Authorization Management Program (FedRAMP) will undergo an abbreviated security review process. Cloud services that are not "FedRAMPed" will undergo a more in-depth security review process. Any cloud service's security level and trustworthiness must match the sensitivity of the data stored on that service. If there are circumstances that fall outside the ability to comply with and/or conform to County policies, an exception waiver may be required.

All cloud computing services must be reviewed and approved by the Chief Information Officer (CIO) or designee before purchase or deployment, including renewals. The CIO or designee has the right to deny the request and shall provide the reason(s) for doing so as well as alternatives so that a mutually agreeable solution can be developed.

The use of cloud computing services shall comply with all current laws and regulations as well as all County policies. All software stored in the cloud must comply with licensing agreements and copyright laws. Additionally, all internet domains (URLs) associated with County business shall be managed and registered through ISD.

24.5. Software as a Service

Software as a Service (SaaS) solutions must utilize latest version of Security Assertion Markup Language (SAML) authentication (WS-Federation and Okta's Secure Web Authentication (SWA) may be used in lieu of SAML) and integrate with the County's identity provider (currently Okta). Multi-factor authentication is required when the application is accessed from outside of the County's network. If solutions do not utilize SAML authentication or multi-factor authentication, a request for exception, signed by the Department Head, must be submitted to the CIO or designee, for approval. Note: The security assessment may result in a request for exception based on the results of the review and is not limited to the above-mentioned authentication processes.

All software must be configured to have a lock-out session after thirty (30) minutes of idle time. Full auditing, in coordination with ISD, must be enabled to allow for successful and unsuccessful account logon events, account management events, and system events. Audit logs, if performed by another organization, shall be shared with the County upon request or as stated in the underlying agreement. All audit logs must be stored for a minimum of one year.

Contingency plans for disaster recovery must be provided by the vendor in all SaaS solutions including a strategy to restore the data within a specified time frame.

Both vendor and County roles and responsibilities shall be clearly stated including enforcement mechanisms to meet the required service levels. All parties must also comply with Administrative Memorandum B-1.

The terms and conditions of termination shall be clearly defined along with the disposal and/or transfer of data.

24.6. Confidential Data

Cloud systems are subject to the same internal standards as those located on-premises. Confidential data may only be stored and managed through a secure vendor.

All vendors shall comply with all County specified standards and requirements in addition to federal and state mandated standards, such as HIPAA. Compliance shall be detailed within the business case for each application. Vendors must provide information regarding the controls they employ to maintain security on all HIPAA and PII data. The following list includes security concerns that will be evaluated in the security review process. Note that an exception waiver may be required in the event that the listed County requirements are not met.

- How and where vendor encrypts data, both at rest and in motion
- How vendor employees who will have physical access to the network and infrastructure that hosts the application, are vetted
- What third-party audits will be/have been performed to validate vendor controls • What security features are and are not included as part of their SLA
- What constitutes a security event and what their notification policies and procedures are after a security event occurs
- If the backups of the County's data are moved offsite, how are they encrypted • How will data be securely deleted or destroyed as requested
- The vendor's ability to provide patches and update products, including the patch schedules and timeline for end-of-device support
- Assurance that the sharing of the County provided account password will be strictly prohibited

Client data from the cloud may not be transmitted to a personal computing device (such as a flash/thumb drive).

24.7. Other County Policies

The County has other policies that address specific areas of information security including policies on IT security, Internet use, email, mobile technology use, vendor/contractor access, and portable computing. These policies are also applicable and extend to cloud services including the use and storage of information. Departments may have internal policies that also address these issues. These policies are cumulative and in the event of conflict, the policies providing the County with the greatest level of security shall apply.

24.8. Responsibility

Departments shall be responsible for providing security awareness and training to all users of devices or electronic media containing Personal Health Information (PHI) or PII as it relates to the HIPAA requirements for all data under their control. ISD will be responsible for providing Countywide security awareness and training.

24.9. Policy Enforcement

The CIO or designee is the policy administrator for information technology resources and will ensure that this process is followed. Additionally, Division Directors, managers, and Department Heads are responsible for compliance with County policies within their respective administrative areas.

Any violations of this policy shall be reported to the CIO or designee. Violations will be investigated and may result in disciplinary action up to and including dismissal from County employment. For violations of patient confidentiality, the procedures of the Patient Confidentiality Sanctions Policy as regulated by HIPAA will apply. Vendors who violate this policy may be subject to contract termination, denial of service, and/or legal penalties, both criminal and civil.

24.10. Revision History

Effective Date	Changes Made
7/31/2018	Policy established
6/22/2020	Policy revised

25. Additional Technology Terms and Conditions

25.1. Disentanglement

Contractor shall cooperate with County and County's other contractors to ensure a smooth transition at the time of termination of this Agreement, regardless of the nature or timing of the termination. Contractor shall cooperate with County's efforts to effectuate such transition with the goal of minimizing or eliminating any interruption of work required under the Agreement and any adverse impact on the provision of services or the County's activities; provided, however, that County shall pay Contractor on a time and materials basis, at the then-applicable rates, for all additional services performed in connection with such cooperation. Contractor shall deliver to County or its designee, at County's request, all documentation and data related to County, including, but not limited to, patient files, held by Contractor, and after return of same, Contractor shall destroy all copies thereof still in Contractor's possession, at no charge to County. Such data delivery shall be in an electronic format to facilitate archiving or loading into a replacement application. County and Contractor shall mutually agree to the specific electronic format.

Upon any termination of the Agreement, regardless of the nature or timing of the termination, County shall have the right, for up to twelve (12) months (the "Transition Period"), at County's option and request, to continue to receive from Contractor all maintenance and support services, at the then-applicable rates provided, however, that the annual support and

maintenance fee shall be prorated and paid in advance on a monthly basis during such time, and the amount of such support and maintenance fee shall remain subject to the limitations set forth in the Agreement regarding any increase in such fee.

25.2. Warranty

This Software is subject to a warranty. Licensor warrants to Licensee that the Software will perform according to the Software's documentation at the time of the implementation and that, to the best of Licensor's knowledge, Licensee's use of this Software according to the documentation is not an infringement of any third party's intellectual property rights. If the Software is subsequently upgraded, repaired or otherwise changed by Licensor, Licensor warrants to Licensee that the Software will continue to perform according to its original documentation as well as according to updated documentation to the extent new features are added. To the extent permitted by law, the above-stated warranty replaces all other warranties, express or implied, and Licensor disclaims all implied warranties including any implied warranty of title, merchantability, or of fitness for a particular purpose. No agent of Licensor is authorized to make any other warranties or to modify this warranty. Licensee is required to inform Licensor of any potential breach of this warranty within one year of identifying any performance defect in the Software that contradicts the expected performance as outlined in the original and/or updated documentation. Licensee will document any such potential breach of warranty and Licensee's remedies by utilizing the Service Level Agreement outlined in the Exhibit C of this agreement.

County represents and warrants that: (a) County has provided all patient privacy notices and obtained any and all authorizations and consents, including any informed consent for use of the Service by Authorized Users and any third party participant in a call conducted through the Service including, without limitation, other healthcare providers, County personnel, consultants, and patient family members ("County Third Parties"), in such form and substance as required by applicable law; (b) County and Authorized Users have all rights in and consents to use and disclose any data transmitted by Authorized Users to the Service, such that the use of such data by Dexterity to fulfill its obligations to County will not violate applicable law or the rights of any third party; (c) County and Authorized Users will comply with all laws applicable to their use of the Service, including those related to privacy, electronic communications, and the provision of and reimbursement for healthcare and telehealth, specifically; (d) use of the Service by County and Authorized Users will not violate or conflict with any agreement or obligation to which County or any Authorized User is subject including, without limitation, any agreement with a government or private insurer or any other third party payer; (e) County is duly authorized to monitor Authorized Users' use of the Service and receive related reporting as part of the Service; (f) to the extent that a professional license or particular certification is required for County or an Authorized User to provide healthcare services, such licenses and certifications will be maintained in effect in each jurisdiction where healthcare services are so provided through use of the Service; and (g) County shall not use URL Scan or similar services to scan or analyze the Service, including but not limited to links, messages, SMS, and content, for any purpose.

26. Health Insurance Portability and Accountability Act (HIPAA)

26.1. DEFINITIONS

Terms used, but not otherwise defined, in this Schedule shall have the same meaning as those terms are defined in 45 Code of Federal Regulations (CFR) sections 160.103, 164.304, and 164.501. All regulatory references in this Schedule are to Title 45 of the Code of Federal Regulations unless otherwise specified.

a. **Business Associate.** "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the parties to this agreement shall mean Contractor.

b. **Covered Entity.** "Covered entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement shall mean County.

c. **HIPAA Rules.** "HIPAA rules" shall mean the Privacy, Security, Breach Notification and Enforcement Rules at 45 CFR part 160 and part 164, as amended and supplemented by Subtitle D of the Health Information Technology for Economic and Clinical Health Act provisions of the American Recovery and Reinvestment Act of 2009.

d. **Designated Record Set.** "Designated Record Set" shall have the same meaning as the term "designated record set" in Section 164.501.

e. **Electronic Protected Health Information.** "Electronic Protected Health Information" (EPHI) means individually identifiable health information that is transmitted or maintained in electronic media; it is limited to the information created, received, maintained or transmitted by Business Associate from or on behalf of Covered Entity.

f. **Individual.** "Individual" shall have the same meaning as the term "individual" in Section 164.501 and shall include a person who qualifies as a personal representative in accordance with Section 164.502(g).

g. **Privacy Rule.** "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E. h. **Protected Health Information.** "Protected Health Information" (PHI) shall have the same meaning as the term "protected health information" in Section 160.103 and is limited to the information created or received by Business Associate from or on behalf of County.

i. **Required By Law.** "Required by law" shall have the same meaning as the term "required by law" in Section 164.103.

j. **Secretary.** "Secretary" shall mean the Secretary of the United States Department of Health and Human Services or his or her designee.

k. **Breach.** The acquisition, access, use, or disclosure of PHI in violation of the Privacy Rule that compromises the security or privacy of the PHI and subject to the exclusions set forth in Section 164.402. Unless an exception applies, an impermissible use or disclosure of PHI *is presumed* to be a breach, unless it can be demonstrated there is a low probability that the PHI has been compromised based upon, at minimum, a four-part risk assessment:

1. Nature and extent of PHI included, identifiers and likelihood of re-identification; 2. Identity of the unauthorized person or to whom impermissible disclosure was made; 3. Whether PHI was actually viewed or only the opportunity to do so existed; 4. The extent to which the risk has been mitigated.

l. **Security Rule.** "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Part 160 and Part 164, Subparts A and C.

m. **Unsecured PHI.** "Unsecured PHI" is protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in relevant HHS guidance.

n. **Security Incident.** "Security Incident" shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system. "Security Incident" includes all incidents that constitute breaches of unsecured protected health information.

26.2. OBLIGATIONS AND ACTIVITIES OF CONTRACTOR AS BUSINESS ASSOCIATE

a. Business Associate agrees to not use or further disclose Protected Health Information other than as permitted or required by the Agreement or as required by law.

b. Business Associate agrees to use appropriate safeguards to comply with Subpart C of 45 CFR part 164 with respect to EPHI and PHI, and to prevent the use or disclosure of the Protected Health Information other than as provided for by this Agreement.

c. Business Associate agrees to make uses and disclosures requests for Protected Health Information consistent with minimum necessary policy and procedures.

d. Business Associate may not use or disclose protected health information in a manner that would violate subpart E of 45 CFR part 164.504 if used or disclosed by Covered Entity.

e. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

f. Business Associate agrees to report to County any use or disclosure of Protected Health Information not authorized by this Agreement.

g. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of County, agrees to adhere to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

h. If Business Associate has Protected Health Information in a Designated Record Set, Business Associate agrees to provide access, at the request of County, and in the time and manner designated by County, to Protected Health Information in a Designated Record Set, to County or, as directed by County, to an Individual in order to meet the requirements under Section 164.524.

i. If Business Associate has Protected Health Information in a Designated Record Set, Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated

Record Set that the County directs or agrees to make pursuant to Section 164.526 at the request of County or an Individual, and in the time and manner designed by County.

j. Business Associate agrees to make internal practices, books, and records relating to the use and disclosure of Protected Health Information received from or created or received by Business Associate on behalf of County, available to the Secretary at the request of the Secretary, in a time and manner designated by the Secretary, for purposes of the Secretary determining County's compliance with the Privacy Rule. Upon request by the Secretary, Business Associate agrees to share any information provided to the Secretary with County.

k. Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for County to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with Section 164.528.

l. Business Associate agrees to provide to County or an Individual in the time and manner designated by County, information collected in accordance with Section (k) of this Schedule, in order to permit County to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with Section 164.528.

m. Business Associate shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of EPHI that Business Associate creates, receives, maintains, or transmits on behalf of County.

n. Business Associate shall conform to generally accepted system security principles and the requirements of the final HIPAA rule pertaining to the security of health information.

o. Business Associate shall ensure that any agent to whom it provides EPHI, including a subcontractor, agrees to implement reasonable and appropriate safeguards to protect such EPHI.

p. Business Associate shall report to County any Security Incident within five (5) business days of becoming aware of such incident. Business Associate shall also facilitate breach notification(s) to the appropriate governing body (i.e., HHS, OCR, etc.) as required by law. As appropriate and after consulting with County, Business Associate shall also notify affected individuals and the media of a qualifying breach.

q. Business Associate understands that it is directly liable under the HIPAA rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of Protected Health Information that are not authorized by this Attachment, the underlying contract as or required by law.

26.3. PERMITTED USES AND DISCLOSURES BY CONTRACTOR AS BUSINESS ASSOCIATE

Except as otherwise limited in this Schedule, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, County as specified in the Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by County.

26.4. OBLIGATIONS OF COUNTY

- a. County shall provide Business Associate with the notice of privacy practices that County produces in accordance with Section 164.520, as well as any changes to such notice.
- b. County shall provide Business Associate with any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, if such changes affect Business Associate's permitted or required uses and disclosures.
- c. County shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that County has agreed to in accordance with Section 164.522.

26.5. PERMISSIBLE REQUESTS BY COUNTY

County shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if so requested by County, unless the Business Associate will use or disclose Protected Health Information for, and if the Agreement provides for, data aggregation or management and administrative activities of Business Associate.

26.6. DUTIES UPON TERMINATION OF AGREEMENT

- a. Upon termination of the Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from County, or created, maintained, or received by Business Associate on behalf of County, that Business Associate still maintains in any form. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.
- b. In the event that Business Associate determines that returning or destroying Protected Health Information is infeasible, Business Associate shall provide to County notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of the Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

26.7. MISCELLANEOUS

- a. **Regulatory References.** A reference in this Schedule to a section in the HIPAA Privacy Rule means the section as in effect or as amended, and for which compliance is required.
- b. **Amendment.** The Parties agree to take such action as is necessary to amend this Schedule from time to time as is necessary for County to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act, Public Law 104-191.
- c. **Survival.** The respective rights and obligations of Business Associate under this Schedule shall survive the termination of the Agreement.
- d. **Interpretation.** Any ambiguity in this Schedule shall be resolved in favor of a meaning that permits County to comply with the Privacy Rule.

e. **Reservation of Right to Monitor Activities.** County reserves the right to monitor the security policies and procedures of Business Associate.

27. Intellectual Property

27.1. Intellectual Property Rights

As between the parties, Contractor exclusively owns and reserves all right, title, and interest in and to the Service, the Contractor's online platform of websites and mobile applications ("Doximity Platform"), and all data relating to Contractors' network of healthcare professional members ("Doximity Members") use thereof, its ideas, know-how, discoveries, inventions, work product, reports, methodologies, processes and procedures, technologies, hardware, software, and all derivatives of the foregoing, and County has no right, license, or authorization with respect to any of the foregoing, except as expressly set forth in this Agreement. Any rights not expressly granted by Contractor are reserved by Contractor. County grants to Contractor a nonexclusive, worldwide, perpetual, irrevocable, transferable, sublicensable, royalty-free, fully paid-up license to use and exploit for any purpose without any further obligation to County any County-provided suggestions, comments or other feedback relating to Contractor Platform or the Service.

28. Personally Identifiable Information

Requirements for County Contractors, Subcontractors, Vendors and Agents

28.1. Definitions

Personally Identifiable Information (PII), or Sensitive Personal Information (SPI), as used in Federal information security and privacy laws, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. PII may only be used to assist in the administration of programs in accordance with 45 C.F.R. § 205.40, *et seq.* and California Welfare & Institutions Code section 10850.

a. **"Assist in the Administration of the Program"** means performing administrative functions on behalf of County programs, such as determining eligibility for, or enrollment in, and collecting context PII for such purposes, to the extent such activities are authorized by law.

b. **"Breach"** refers to actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to context PII, whether electronic, paper, verbal, or recorded.

c. **"Contractor"** means those contractors, subcontractors, vendors and agents of the County performing any functions for the County that require access to and/or use of PII and that are authorized by the County to access and use PII.

d. **"Personally Identifiable Information" or "PII"** is personally identifiable information that can be used alone, or in conjunction with any other reasonably available information, to identify a specific individual. PII includes, but is not limited to, an individual's name, social security number, driver's license number, identification number, biometric records, date of birth, place of birth, or mother's maiden name. PII may be electronic, paper, verbal, or recorded.

e. **“Security Incident”** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PII, or interference with system operations in an information system which processes PII that is under the control of the County or County’s Statewide Automated Welfare System (SAWS) Consortium, or under the control of a contractor, subcontractor or vendor of the County, on behalf of the County.

f. **“Secure Areas”** means any area where:

i. Contractors administer or assist in the administration of County programs; ii. PII is used or disclosed; or

iii. PII is stored in paper or electronic format.

28.2. Restrictions on Contractor re Use and Disclosure of PII

a. Contractor agrees to use or disclose PII only as permitted in this Agreement and only to assist in the administration of programs in accordance with 45 CFR § 205.50, *et seq.* and California Welfare & Institutions Code section 10850 or as otherwise authorized or required by law. Disclosures, when authorized or required by law, such as in response to a court order, or when made upon the explicit written authorization of the individual, who is the subject of the PII, are allowable. Any other use or disclosure of PII requires the express approval in writing by the County. No Contractor shall duplicate, disseminate or disclose PII except as allowed in this Agreement.

b. Contractor agrees to only use PII to perform administrative functions related to the administration of County programs to the extent applicable.

c. Contractor agrees that access to PII shall be restricted to Contractor’s staff who need to perform specific services in the administration of County programs as described in this Agreement.

d. Contractor understands and agrees that any of its staff who accesses, discloses or uses PII in a manner or for a purpose not authorized by this Agreement may be subject to civil and criminal sanctions available under applicable Federal and State laws and regulations.

28.3. Use of Safeguards by Contractor to Protect PII

a. Contractor agrees to ensure that any agent, including a subcontractor, to whom it provides PII received from, or created or received by Contractor on behalf of County, agrees to adhere to the same restrictions and conditions contained in this Attachment PII.

b. Contractor agrees to advise its staff who have access to PII, of the confidentiality of the information, the safeguards required to protect the information, and the civil and criminal sanctions for non-compliance contained in applicable Federal and State laws and regulations.

c. Contractor agrees to train and use reasonable measures to ensure compliance by Contractor’s staff, including, but not limited to (1) providing initial privacy and security awareness training to each new staff within thirty (30) days of employment; (2) thereafter, providing annual refresher training or reminders of the PII privacy and security safeguards to all Contractor’s staff; (3) maintaining records indicating each Contractor’s staff name and the date on which the privacy and security awareness training was completed; and (4) retaining training records for a period of three (3) years after completion of the training.

- d. Contractor agrees to provide documented sanction policies and procedures for Contractor's staff who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment when appropriate.
- f. Contractor agrees to conduct a background check of Contractor's staff before they may access PII. Contractor further agrees that screening documentation shall be retained for a period of three (3) years following conclusion of the employment relationship.
- g. Contractor agrees to conduct periodic privacy and security reviews of work activity, including random sampling of work product by Contractor's staff by management level personnel who are knowledgeable and experienced in the areas of privacy and information security in the administration of County's programs and the use and disclosure of PII. Examples include, but are not limited to, access to data, case files or other activities related to the handling of PII.
- h. Contractor shall ensure that PII is used and stored in an area that is physically safe from access by unauthorized persons at all times and safeguard PII from loss, theft, or inadvertent disclosure by securing all areas of its facilities where Contractor's staff assist in the administration of the County's programs and use, disclose, or store PII.
- i. Contractor shall ensure that each physical location, where PII is used, disclosed, or stored, has procedures and controls that ensure an individual who is terminated from access to the facility has access revoked.
- j. Contractor shall ensure that there are security guards or a monitored alarm system at all times at Contractor's facilities and leased facilities where five hundred (500) or more individually identifiable records of PII is used, disclosed, or stored. Video surveillance systems are recommended.
- k. Contractor shall ensure that data centers with servers, data storage devices, and/or critical network infrastructure involved in the use, storage, and/or processing of PII have perimeter security and physical access controls that limit access to only those authorized by this Agreement. Visitors to any Contractor data centers area storing PII as a result of administration of a County program must be escorted at all times by authorized Contractor's staff.
- l. Contractor shall have policies that include, based on applicable risk factors, a description of the circumstances under which Contractor staff can transport PII, as well as the physical security requirements during transport.
- m. Contractor shall ensure that any PII stored in a vehicle shall be in a non-visible area such as a trunk, that the vehicle is locked, and under no circumstances permit PII be left unattended in a vehicle overnight or for other extended periods of time.
- n. Contractor shall ensure that PII shall not be left unattended at any time in airplanes, buses, trains, etc., including baggage areas. This should be included in training due to the nature of the risk.
- o. Contractor shall ensure that all workstations and laptops, which use, store and/or process PII, must be encrypted using a FIPS 140-2 certified algorithm 128 bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk. It is encouraged, when available and when feasible, that the encryption be 256 bit.

- p. Contractor shall ensure that servers containing unencrypted PII must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review. It is recommended to follow the guidelines documented in the latest revision of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.
- q. Contractor agrees that only the minimum necessary amount of PII required to perform required business functions will be accessed, copied, downloaded, or exported.
- r. Contractor shall ensure that all electronic files, which contain PII data is encrypted when stored on any mobile device or removable media (i.e. USB drives, CD/DVD, smartphones, tablets, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm 128 bit or higher, such as AES. It is encouraged, when available and when feasible, that the encryption be 256 bit.
- s. Contractor shall ensure that all workstations, laptops and other systems, which process and/or store PII, must install and actively use an antivirus software solution. Antivirus software should have automatic updates for definitions scheduled at least daily. In addition, Contractor shall ensure that:
- i. All workstations, laptops and other systems, which process and/or store PII, must have critical security patches applied, with system reboot if necessary.
 - ii. There must be a documented patch management process that determines installation timeframe based on risk assessment and vendor recommendations.
 - iii. At a maximum, all applicable patches deemed as critical must be installed within thirty (30) days of vendor release. It is recommended that critical patches which are high risk be installed within seven (7) days.
 - iv. Applications and systems that cannot be patched within this time frame, due to significant operational reasons, must have compensatory controls implemented to minimize risk.
- t. Contractor shall ensure that all of its staff accessing Personally Identifiable Information on applications and systems will be issued a unique individual password that is a least eight (8) characters, a non-dictionary word, composed of characters from at least three (3) of the following four (4) groups from the standard keyboard: upper case letters (A-Z); lower case letters (a-z); Arabic numerals (0-9) and special characters (!, @, #, etc.). Passwords are not to be shared and changed if revealed or compromised. All passwords must be changed every (90) days or less and must not be stored in readable format on the computer or server.
- u. Contractor shall ensure that usernames for its staff authorized to access PII will be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee within twenty- four (24) hours. Note: Twenty-four (24) hours is defined as one (1) working day.
- v. Contractor shall ensure when no longer needed, all PII must be cleared, purged, or destroyed consistent with NIST SP 800-88, Guidelines for Media Sanitization, such that the Personally Identifiable Information cannot be retrieved.

w. Contractor shall ensure that all of its systems providing access to PII must provide an automatic timeout, requiring re-authentication of the user session after no more than twenty (20) minutes of inactivity.

x. Contractor shall ensure that all of its systems providing access to PII must display a warning banner stating, at a minimum that data is confidential; systems are logged, systems use is for business purposes only by authorized users and users shall log off the system immediately if they do not agree with these requirements.

y. Contractor will ensure that all of its systems providing access to PII must maintain an automated audit trail that can identify the user or system process which initiates a request for PII or alters PII. The audit trail shall be date and time stamped; log both successful and failed accesses be read-access only; and be restricted to authorized users. If PII is stored in a database, database logging functionality shall be enabled. The audit trail data shall be archived for at least three (3) years from the occurrence.

z. Contractor shall ensure that all of its systems providing access to PII shall use role-based access controls for all user authentications, enforcing the principle of least privilege.

aa. Contractor shall ensure that all data transmissions of PII outside of its secure internal networks must be encrypted using a Federal Information Processing Standard (FIPS) 140-2 certified algorithm that is 128 bit or higher, such as Advanced Encryption Standard (AES) or Transport Layer Security (TLS). It is encouraged, when available and when feasible, that 256-bit encryption be used. Encryption can be end to end at the network level, or the data files containing PII can be encrypted. This requirement pertains to any type of PII in motion such as website access, file transfer, and email.

bb. Contractor shall ensure that all of its systems involved in accessing, storing, transporting, and protecting PII, which are accessible through the Internet, must be protected by an intrusion detection and prevention solution.

cc. Contractor shall ensure that audit control mechanisms are in place. All Contractor systems processing and/or storing Personally Identifiable Information must have a least an annual system risk assessment/security review that ensure administrative, physical, and technical controls are functioning effectively and provide an adequate level of protection. Review shall include vulnerability scanning tools.

dd. Contractor shall ensure that all of its systems processing and/or storing PII must have a process or automated procedure in place to review system logs for unauthorized access.

ee. Contractor shall ensure that all of its systems processing and/or storing PII must have a documented change control process that ensures separation of duties and protects the confidentiality, integrity and availability of data.

ff. Contractor shall establish a documented plan to enable continuation of critical business processes and protection of the security of PII kept in an electronic format in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than twenty-four (24) hours.

gg. Contractor shall ensure its data centers with servers, data storage devices, and critical network infrastructure involved in the use, storage and/or processing of PII, must include environmental protection such as cooling, power, and fire prevention, detection, and suppression.

hh. Contractor shall establish documented procedures to backup PII to maintain retrievable exact copies of PIII. The documented backup procedures shall contain a schedule which includes incremental and full backups, storing backups offsite, inventory of backup media, recovery of PII data, an estimate of the amount of time needed to restore PII data.

ii. Contractor shall ensure that PII in paper form shall not be left unattended at any time, unless it is locked space such as a file cabinet, file room, desk or office. Unattended means that information may be observed by an individual not authorized to access the information. Locked spaces are defined as locked file cabinets, locked file rooms, locked desks, or locked offices in facilities which are multi-use, meaning that there are Contractor's staff and non-Contractor functions in one building in work areas that are not securely segregated from each other. It is recommended that all PII be locked up when unattended at any time, not just within multi-use facilities.

jj. Contractor shall ensure that any PII that must be disposed of will be through confidential means, such as crosscut shredding or pulverizing.

kk. Contractor agrees that PII must not be removed from its facilities except for identified routine business purposes or with express written permission of the County.

ll. Contractor shall ensure that faxes containing PII shall not be left unattended and fax machines shall be in secure areas. Faxes containing PII shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them and notify the sender. All fax numbers shall be verified with the intended recipient before send the fax.

mm. Contractor shall ensure that mailings containing PII shall be sealed and secured from damage or inappropriate viewing of PII to the extent possible. Mailings that include five hundred (500) or more individually identifiable records containing PII in a single package shall be sent using a tracked mailing method that includes verification of delivery.

28.4. Reporting of Breaches Required by Contractor to County; Mitigation

a. Contractor shall report to County within five (5) days of discovery, to the County contact listed in this agreement by email or telephone as listed in the of unsecured PII, if that PII was, or is, reasonably believed to have been accessed or acquired by an unauthorized person, any actual security incident, intrusion or unauthorized access, use or disclosure of PII in violation of this Agreement, or actual loss of confidential data affecting this Agreement.

b. Contractor understands that State and Federal Law requires a breaching entity to notify individuals of a breach or unauthorized disclosure of their PII. Contractor shall ensure that said notifications shall comply with the requirements set forth in California Civil Code section 1798.29, and 42 U.S.C. section 17932, and its implementing regulations, including but not limited to, the requirement that the notifications be made without unreasonable delay and in no event later than sixty (60) calendar days.

c. Contractor agrees to promptly mitigate, to the extent practicable, any harmful effect that is known to Contractor stemming from a use or disclosure of PII in violation of the requirements of this Agreement, including taking any action pertaining to such use or disclosure required by applicable Federal and State laws and regulations.

28.5. Permitted Uses and Disclosures of PII by Contractor

Except as otherwise limited in this schedule, Contractor may use or disclose PII to perform functions, activities, or services for, or on behalf of, County as specified in the Agreement; provided that such use or disclosure would not violate the Privacy Rule if done by County.

28.6. Obligations of County

a. County shall provide Contractor with the notice of privacy practices that County produces in accordance with California Welfare and Institutions Code section 10850, as well as any changes to such notice.

b. County shall notify Contractor of any changes in, or revocation of, permission by Individual to use or disclose PII, if such changes affect Contractor's permitted or required uses and disclosures.

c. County shall notify Contractor of any restriction to the use or disclosure of PII that County has agreed to in accordance with California Welfare and Institutions Code section 10850.

28.7. Permissible Requests by County

County shall not request Contractor to use or disclose PII in any manner that would not be permissible under the Privacy Rule if so requested by County, unless Contractor will use or disclose PII for, and if the Agreement provides for, data aggregation or management and administrative activities of Contractor.

28.8. Duties Upon Termination of Agreement

a. Upon termination of the Agreement, for any reason, Contractor shall return or destroy all PII received from County, or created, maintained, or received by Contractor on behalf of County that Contractor still maintains to perform the Service. This provision shall apply to PII that is in the possession of subcontractors or agents of Contractor. Contractor shall retain no copies of the PII for this Service.

b. In the event that Contractor determines that returning or destroying PII is infeasible, Contractor shall provide to County notification of the conditions that make return or destruction infeasible. Upon mutual Agreement of the Parties that return or destruction of PII is infeasible, Contractor shall extend the protections of the Agreement to such PII and limit further uses and disclosures of such PII to those purposes that make the return or destruction infeasible, for so long as Contractor maintains such PII.

28.9. Miscellaneous

a. **Regulatory References.** A reference in this Attachment to a section in the Personally Identifiable Information Privacy Rule means the section as in effect or as amended, and for which compliance is required.

b. **Amendment.** The Parties agree to take such action as is necessary to amend this Schedule from time to time as is necessary for County to comply with the requirements of the Privacy

Rule and in accordance 45 CFR § 205.40, *et seq.* and California Welfare and Institutions Code section 10850.

c. **Survival.** The respective rights and obligations of Contractor under this Attachment shall survive the termination of the Agreement unless and until the PII is destroyed or returned to the County.

d. **Interpretation.** Any ambiguity in any provision in this Attachment shall be resolved in favor of a meaning that permits County to comply with the Privacy Rule.

e. **Reservation of Right to Monitor Activities.** County reserves the right to monitor the security policies and procedures of Contractor.

29. Rehabilitation Act of 1973

The undersigned (hereinafter called "Contractor(s)") hereby agrees that it will comply with Section 504 of the Rehabilitation Act of 1973, as amended, all requirements imposed by the applicable DHHS regulation, and all guidelines and interpretations issued pursuant thereto.

The Contractor(s) gives/give this assurance in consideration of for the purpose of obtaining contracts after the date of this assurance. The Contractor(s) recognizes/recognize and agrees/agree that contracts will be extended in reliance on the representations and agreements made in this assurance. This assurance is binding on the Contractor(s), its successors, transferees, and assignees, and the person or persons whose signatures appear below are authorized to sign this assurance on behalf of the Contractor(s).

The Contractor(s): (Check a or b)

☐ a. Employs fewer than 15 persons.

☒ b. Employs 15 or more persons and, pursuant to section 84.7 (a) of the regulation (45 C.F.R. 84.7 (a), has designated the following person(s) to coordinate its efforts to comply with the DHHS regulation.

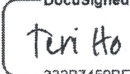
Name of 504 Person: Teri Ho

Name of Contractor(s): Street 500 3rd Street, Suite 510, San Francisco, CA 94107

Address or P.O. Box: City, State, 500 3rd Street, Suite 510, San Francisco, CA 94107

Zip Code: 94107

I certify that the above information is complete and correct to the best of my knowledge

Signature:  DocuSigned by:
332B7459BE4E417...

Title of Authorized Official: Director of Revenue

Date: March 27, 2025

*Exception: DHHS regulations state that: "If a recipient with fewer than 15 employees finds that, after consultation with a disabled person seeking its services, there is no method of complying with (the facility accessibility regulations) other than making a significant alteration in its existing facilities, the recipient may, as an alternative, refer the handicapped person to other providers of those services that are accessible."

SIGNATURE PAGE TO FOLLOW

In witness of and in agreement with this Agreement's terms, the parties, by their duly authorized representatives, affix their respective signatures:

For Contractor: Doximity, Inc

DocuSigned by:

Teri Ho
Contractor Signature

March 27, 2025
Date

Teri Ho
Contractor Name (please print)

Director of Revenue
Contractor Title (please print)

COUNTY OF SAN MATEO

By: Dan J. Conner Resolution No. 081123
President, Board of Supervisors, San Mateo County

Date: May 6, 2025

ATTEST:

By: Phil Gallagher
Clerk of Said Board

Exhibit A Scope of Work

In consideration of the payments set forth in Exhibit B, Contractor shall provide the following services:

Dialer Enterprise - is a communication service that enables Authorized Users to initiate and conduct secure voice and video calls with their patients from their mobile device or computer. Authorized Users will have access to the following Dialer.

Amion Enterprise Services – is a Cloud-based scheduling software allowing users to build and view schedules using our on-cloud platform.

DIALER ENTERPRISE DESCRIPTION

Below is a description of the Dialer Enterprise Service. Doximity may modify the Service as it deems appropriate from time to time, provided that in no event will any such modification materially degrade the quality or functionality of the Service during the then-current Term.

1. **Dialer Enterprise** – Dialer Enterprise is a communication service that enables Authorized Users to initiate and conduct secure voice and video calls with their patients from their mobile device or computer. Authorized Users will have access to the following Dialer Enterprise features:
 - A. **Unlimited usage**
 - Authorized Users will not be subject to any usage limits
 - B. **Group calling capabilities**
 - Authorized Users will have the ability to conduct a Dialer Enterprise video call with more than 2 participants
 - C. **Engagement and utilization reporting**
 - Doximity will make available to Client aggregate monthly engagement reports. Custom reporting is available for an additional fee, as agreed upon in a separate Statement of Work form.
 - D. **Future features exclusive to Dialer Enterprise**
 - Doximity will endeavor to develop additional features for Dialer Enterprise that build upon its existing capabilities

AMION ENTERPRISE SERVICE DESCRIPTION

Below is a description of the Amion Service for which Client has purchased a subscription pursuant. We may modify the Service, and any component thereof, as we deem appropriate from time to time, provided that in no event will any such modification materially degrade the quality or functionality of the Service during the then-current Term.

1. AMiON Enterprise Scheduling Software & Support

Cloud-based scheduling software allowing users to build and view schedules using our on-cloud platform.

- **Unlimited User Licenses** (Unless otherwise specified in the Order Form)- Our enterprise solution offering includes unlimited user licenses for users at your organization's existing facilities. Users will not be subject to any usage limits or licensing fees for users to edit and view your organization's Amion schedules.
- **Amion Mobile App** - Unlimited access to Amion mobile app to make on-the-fly schedule updates and allow users to view schedules anywhere, anytime.
- **Master Central Display** - Central display of all Client schedules to serve as a single source of truth for streamlined visibility and communication.
- **Specialty/Department Schedules** - Unlimited schedules for your organization's existing hospitals, clinics and facilities.
- **VIP Support** - VIP support for all Amion system support issues submitted via phone and email.
- **Client Success Management** - Access to a designated Client Success Manager (CSM) to serve as your primary point of contact for advanced issue resolution, monitoring of organizational progress and communication of AMiON advanced features.
- **Training Library** - Access to library of pre-recorded training and user guides for all Amion functionality.

Exhibit A-1
Implementation
Scope of Work

Dialer Enterprise Implementation Services – Scope of Work

User Provisioning

Doximity will enable access to Dialer for all Authorized Users

Clinician training

During the applicable Subscription Term and no more frequently than annually upon Client's request, Doximity will provide remote online Dialer Enterprise training to Client's clinical team at a mutually agreeable time and manner.

Physician promotion

Doximity will provide Client materials promoting Doximity registration and engagement, e.g., email templates, articles, and brochures, that Client may distribute to clinicians affiliated with the Client's institution.

AMiON Implementation Services – Scope of Work

Support to implement and train schedulers on Amion's scheduling software leveraging system best practices.

- **AMiON Implementation Management** - Dedicated Amion Implementation Manager to guide your organization through the implementation process.
- **AMiON Training** - Specialized training for your Enterprise Administrator, Super Users and Schedulers on AMiON schedule build and functionality via AMiON Academy.
- **SSO & Epic Integration**
 - **Single-Sign On (SSO)** - Leverage your active directory to allow Users to log in and access Amion schedules with their organizational credentials.
 - **AMiON to Epic Integration** - View and contact providers from Amion schedules directly within Epic.

Additional Implementation Services Offerings:

- **AMiON Build/Training Resources** – Doximity offers additional implementation resources for system build and end-user training at a competitive hourly-based pricing model.

AMION ENTERPRISE IMPLEMENTATION SERVICES

1. Engagement Overview

Doximity will partner with Client to provide standard implementation services for the facility outlined in the 'Services Purchased' section above. The AMiON Implementation services include: (1) an Implementation Manager to help guide Client through the implementation and (2) specialized AMiON training & build support. Doximity's methodology is rooted in system best practices and years of experience, allowing our team to effectively address challenges, mitigate risks, and deliver measurable results. Epic and SSO integrations only apply if purchased on the Order Form.

1.1. Assumptions

1. Implementation Services to begin at First Production Use of the services.
2. Implementation Services not to exceed a maximum of 4 weeks in duration from planning to implementation kick-off and 16 weeks in duration from implementation kick-off date to go-live. If the implementation is not completed within this timeframe, an additional Order Form will need to be executed to cover extended Implementation support.
3. The Epic On-Call Finder and SSO integrations apply to the facility identified in the "Fee Schedule" and are included in the price of the implementation services as long as they are completed in conjunction with the AMiON implementation during the designated timeframe outlined above. If integrations are completed after Year 1 the parties will mutually agree on additional pricing and scope via a new Statement of Work.
4. Client will identify key stakeholders including an Executive Sponsor, Enterprise AMiON Administrator, Project Manager and a minimum of two (2) Super-Users per facility. These stakeholders will be made available to meet at a cadence as outlined in the project plan, and the kickoff will not be scheduled until these roles are filled. Delays may result in changes to project timelines and fees.
5. We will support the implementation process virtually. Onsite support can be provided at Client request and support and travel costs will be invoiced separately. All travel will follow the Reimbursable Travel Expenses of this agreement.
6. Any changes to scope, client resourcing, and/or timelines will require an additional amendment to be executed to cover additional Implementation support and fees.
7. AMiON Training Sessions are available to be scheduled during weekday daytime hours (Monday through Friday from 8:00 am - 5:00 pm CT) excluding Doximity designated holidays.
8. Scope Expansion: Client agrees that if an event occurs that will materially increase the number of schedules and/or scope of Services, such as acquisition of new hospital, clinic or other new facility; Client will notify Doximity in writing of such an event no later than 90 days prior to the effective date of such event so that Client's scope and support needs can be reviewed. In the event of such change, adjustments to pricing and/or schedule licensing will apply and the parties will execute a new Order Form.

2. **Timeline (16 weeks)**

Doximity follows a comprehensive multi-phased approach to guide clients through the AMiON implementation process. Below is an overview of our methodology and explanation of each phase.

2.1. Phase 1: Planning

The planning phase focuses on defining project objectives, scope, timelines, resources and system integration requirements. This time allows us to establish relationships with key stakeholders and sets the foundation for the project's successful execution by providing clarity, direction, and alignment among all parties involved. This phase includes an initial training for super users, key stakeholders and executive sponsors.

- **AMiON Administrator Training (Admin 101):** Focuses on establishing enterprise build standards, viewing AMiON schedules, determining preferred communication methods and process for commissioning/decommissioning schedules, call assignments and resources.

2.2. Phase 2: Initiation & Training

The purpose of the initiation & training phase is to officially kick off the AMiON Implementation Project and set the stage for its successful execution. The phase begins by bringing together key stakeholders, defined AMiON super users and relevant individuals to establish a shared understanding of the project's objectives, scope, roles and responsibilities and expectations. Post project kickoff, we will educate your organization's Super Users & Schedulers in AMiON's scheduling tools while leveraging the enterprise build standards established in the planning phase. Your organization will have full access to AMiON's self-service training platform - Amion Academy. Within the Academy, your staff will have access to the following:

- **Learning Paths:** short, engaging video modules to introduce you to the scheduling software. Learning Path Options include:
 - Creating a New Provider Schedule
 - Taking Over an Existing Provider Schedule
 - Residency and Fellowship Scheduling
- **Training Guides:** step-by-step instructions for building and maintaining Amion schedules including: (1) best practices, (2) tips and tricks, and (3) build considerations.
 - Intro to AMiON Scheduling (Scheduling 101)
 - AMiON Enterprise Administrator Guide (Admin 101)
 - AMiON Switchboard User Training Guide (Switch 101)
 - AMiON to Epic Integration Setup and Support Guide
- **Training Topics/Tip Sheets:** specialized setup and support training documents tailored to specific AMiON scheduling functionality.

2.3. Phase 3: Build & Testing

The build & testing phase allows time for Client to complete all AMiON schedule build and testing. The AMiON Implementation Manager will facilitate weekly project team meetings to review project status, discuss any risks/issues and be available to answer questions regarding system build.

Single-Sign On (SSO) and Epic Integration - During this time, the AMiON Implementation Manager will partner with Client's IT/Active Directory and Epic team members to establish and test the SSO and Epic system integrations with AMiON.

2.4. Phase 4: End-User Adoption & Readiness

When introducing a new software to an organization, one of the critical success factors for its success is the user adoption rate. Doximity will partner with Client's training/communication coordinator to develop an End-User Adoption and Communication plan empowering users and ensuring they are equipped with the knowledge and skills necessary to maximize user acceptance and proficiency.

A key milestone of this phase is a Go/No-Go meeting led by the AMiON Implementation Manager prior to go-live to ensure your organization is ready to begin using the AMiON software.

2.5. Phase 5: Go-Live & Stabilization

This phase begins with officially launching the utilization of AMiON on-call schedules at your organization. After go-live, we transition into stabilization. The AMiON Implementation Manager will introduce your organization's enterprise administrator and super users to their Amion Client Success Manager (CSM). The role of your CSM is to act as Client's primary contact regarding AMiON functionality, communicate new features and serve as an escalation contact as needed.

2.6. Roles and Responsibilities

To facilitate mutual success, we have defined key roles and responsibilities for Client, for Doximity, and those shared by both. This matrix is not an all-inclusive list of involved parties and their corresponding duties but rather a tool to help establish expectations prior to beginning the implementation.

2.7. Client Resources

Role	Responsibilities	Engagement
------	------------------	------------

Executive Sponsor	<ul style="list-style-type: none"> ● Overall client sponsor of the Amion implementation ● Sign off on finalized scope and timelines ● Serve as a champion for change throughout the project ● Escalation point for both client and Amion resources ● Participate in key meetings including Project Kickoff and Implementation to Support Transition ● Able to meet as needed to discuss project risks and issues 	1 hr/week
<p>Enterprise Administrator</p> <p>AMiON Resourcing Recommendation: minimum of two (2) per organization.</p>	<ul style="list-style-type: none"> ● Act as project champion. ● Review and approve finalized scope and implementation deliverables. ● Define Client's foundation build, best practices, and project resources. ● Post-Implementation, partner with Amion CSM (Client Success Manager) and serve as primary contact for new AMiON features/functionality, and issue escalations. ● Participate in AMiON Administrator Training (Admin 101) ● Post-Implementation, participate in standing meetings with the Amion CSM (Client Success Manager) to learn about new AMiON features/functionality and discuss project status and issue escalations. 	1-2 hours/week
Project Manager	<ul style="list-style-type: none"> ● Serve as primary Client contact for scheduling meetings and sessions. ● Set expectations appropriately with Client project team members regarding their participation. ● Encourage participation in AMiON team meetings and training sessions. ● Escalate issues/risks to the AMiON Implementation Manager. 	2-4 hours/week

<p>Super User(s)</p> <p>AMiON Resourcing Recommendation: minimum of two (2) per facility.</p>	<ul style="list-style-type: none"> • Act as client SME (subject matter expert) regarding AMiON functionality and specialized build features for scheduling staff and end users. • Train Client schedulers, as needed, on AMiON functionality to successfully build and maintain Client schedules. • Partner with schedulers to build/maintain Client schedules. • Ensure Client enterprise standards are being followed. 	<p>2-4 hours/week</p> <p>*2 hours per schedule for foundation build and development.</p>
<p>Schedulers</p>	<ul style="list-style-type: none"> • Build and maintain Client schedules. • Follow enterprise build standards. • Communicate release of schedules and schedule updates to end-users. 	<p>2-4 hours/week</p> <p>*2 hours per schedule for foundation build and development.</p>
<p>Switchboard Users</p>	<ul style="list-style-type: none"> • Complete “on-the-fly” schedule updates as needed. 	<p>2 hours total</p>
<p>SSO/Active Directory Analyst</p> <p>(SSO Integration Only)</p>	<ul style="list-style-type: none"> • Act as SME (subject matter expert) regarding your Client’s active directory set-up and primary contact for questions/concerns. • Complete Single Sign-On build and testing. 	<p>1-2 hours/week</p>
<p>Communication Coordinator</p>	<ul style="list-style-type: none"> • Coordinate and manage all internal communication to client end users regarding AMiON on-call functionality and on-call communication processes as part of the AMiON implementation. 	<p>1-2 hours/week</p>

Epic Analyst and Security Analyst (Epic Integration Only)	<ul style="list-style-type: none">• Act as SME (subject matter expert) regarding Epic's On-call Finder and SER master file and primary contact for questions/concerns.• Partner with the AMiON Super Users to complete all SER, Team and Role record mapping within AMiON as part of the Epic integration.• Complete batch job build in Epic to automatically pull flat file data from AMiON.	1-2 hours/week
--	---	----------------

2.8. Doximity Resources

Role	Responsibilities
Implementation Manager	<ul style="list-style-type: none">• Act as AMiON Implementation Project champion.• Guide Client through the implementation process and project plan.• Assist with defining and establishing AMiON foundation best practices.• Conduct AMiON Enterprise Administrator and Scheduler training sessions.• Facilitate weekly project status meetings and answer questions regarding initial schedule build.
Client Success Manager (CSM)	<ul style="list-style-type: none">• Serve as primary contact post implementation.• Communicate AMiON software features and optimizations to client enterprise administrator(s) and super-users.
Support Center Staff	<ul style="list-style-type: none">• First line of support via phone or email for AMiON schedule access issues and error messages.

3. Key Meetings

Communication throughout the implementation is a critical component to success. Our goal throughout any implementation is to provide the Client with the tools and knowledge to independently support their Amion schedules in the long-term. We have found the following meeting schedule supports that goal so the table below outlines key meetings that will occur in each phase of the project along with the applicable client attendees and meeting facilitator.

Phase	Meeting	Description	Client Attendees
-------	---------	-------------	------------------

Phase 1: Planning	Planning Meeting	Review project objectives, scope and timelines, identify client project resources, define enterprise build standards and review system integration requirements. Facilitator: Doximity IM	Executive Sponsor, PM, and Administrator(s).
Phase 1: Planning	Project Kick Off Meeting	Review project scope and timelines, communicate roles/responsibilities and expectations as a participant in the project, discuss key project team meetings, and review the training process and next steps. Facilitator(s): Client PM and Executive Sponsor	Executive Sponsor, PM, Administrator(s), Super User(s), and Schedulers.
Phase 2: Initiation and Training	Epic Integration Kick Off Meeting (Epic Integration Only)	Review Amion to Epic Integration process, define Epic project resources, and establish integration standards. Facilitator: Doximity IM and Client PM	Executive Sponsor, PM, Administrator(s), Super User(s), Schedulers and Epic Resources.
Phase 2: Initiation and Training	Single Sign On (SSO) Kick Off Meeting (SSO Integration Only)	Review process for accessing Amion via SSO, identify resources, review timelines and discuss SSO testing process. Facilitator: Doximity IM	PM and SSO Resources. Optional: Executive Sponsor
All Phases	Project Leadership Meeting	Review project status & timelines, discuss risks/issues and develop mitigation/resolution plans (owners, due dates and next steps), provide ongoing education based on project phase, and ensure all project leaders are receiving the same message at the same time. Facilitator(s): Doximity IM and Client PM	Executive Sponsor, PM, Administrator(s), Super User(s), and Schedulers.
Phase 2 through Go-live	Project Team Meeting	Provide updates on project status, align team on project goals, communicate expectations and processes, allow for Q&A, ensure Enterprise Build Standards are being	Executive Sponsor, PM, Administrator(s), Super User(s),

		<p>followed, and allow time for training/questions.</p> <p>Facilitator: Client PM</p>	<p>Schedulers and Epic Resources.</p>
<p>Phase 5: Stabilization</p>	<p>Support Transition Meeting</p>	<p>Introduce client to their Doximity support team, review support plan, discuss incident ticket submission process and finalize escalation path and contacts.</p> <p>Facilitator: Doximity CSM</p>	<p>Executive Sponsor, PM, and Administrator(s).</p>

Exhibit B
Payments

In consideration of the services provided by Contractor described in Exhibit A and subject to the terms of the Agreement, County shall pay Contractor based on the following fee schedule and terms:

Services	Year 1	Year 2	Year 3	Year 4	Year 5	Subtotal
Dialer Enterprise	\$35,000	\$35,000	\$35,000	\$35,000	\$35,000	\$175,000
Amion Enterprise Services	\$65,000	\$65,000	\$65,000	\$65,000	\$65,000	\$325,000
Implementation (Year 1 Only)	\$50,000					\$50,000
Contingency Funds*:						\$125,000
Total – Not to Exceed:						\$675,000

*Contingency Funds must follow change management outlined within the agreement.

Exhibit C
Service Level Agreement

a. Contractor ("Doximity") guarantees that the Service's functionality will be available 99.5% of each full calendar month during each full calendar year of the Subscription Term ("Monthly Uptime Percentage Threshold"). If during any such calendar month, actual availability falls below 99.5%, then County ("Client") will be eligible to receive a cash payment equal to 10% of the Subscription Fee it paid in for that month, e.g., a 12-month Subscription Fee will be equally prorated over the associated 12-month Subscription Term, ("Service Credit") subject to Client's compliance with the following process: to receive a Service Credit, Client must submit a request to Doximity Support at support@doximity.com within thirty (30) days from the last day of the calendar month for which Client claims that Doximity failed to meet the Monthly Uptime Percentage Threshold, and provide reasonable details as to the basis for the claim. Doximity reserves the right to verify the validity of the claim. Each Service Credit issued to Client may be applied to future amounts payable by Client to Doximity for the Service. Any Service Credits that are not used within one (1) year following issuance will expire. No refunds or cash value will be provided.

b. Notwithstanding the foregoing, Doximity will not be responsible for unavailability (i) caused by factors beyond Doximity's reasonable control, including, without limitation, telecommunications provider-related problems or issues, Internet access or related problems occurring beyond the point in the network where Doximity maintains access and control over the Service; (ii) to the extent resulting from actions or inactions of Client, Authorized Users or any third party (except for Doximity's agents and subcontractors); (iii) to the extent resulting from Client's or Authorized Users' equipment, software or other technology, third party equipment, software or other technology (except for equipment within Doximity's direct control); (iv) occurring during Doximity's emergency maintenance (maintenance that is necessary for purposes of maintaining the integrity or operation of the Service), regardless of the notice provided by Doximity; or (vi) resulting from any beta services that are not otherwise generally available to Doximity's customers. The Service Credit states Doximity's liability to Client for any failure of Doximity to meet the Monthly Uptime Percentage Threshold.