

September 1, 2026

Board of Supervisors
Kern County Administrative Center
1115 Truxtun Avenue
Bakersfield, CA 93301

**PROPOSED AGREEMENT WITH CASO DOCUMENT MANAGEMENT, INC. TO PROVIDE
COMPREHENSIVE SOFTWARE SOLUTIONS FOR DOCUMENT SCANNING, ELECTRONIC DOCUMENT
MANAGEMENT, AND CONTRACT LIFE CYCLE MANAGEMENT SERVICES
(Fiscal Impact: RFP; \$2,000,000; State/Federal; Budgeted; Discretionary)**

Behavioral Health and Recovery Services (BHRS) requests the approval of an agreement with CASO Document Management, Inc. to provide comprehensive software solutions for document scanning, electronic document management, and contract lifecycle management for the Department from September 1, 2026, through August 31, 2031, in an amount not to exceed \$2,000,000.

Under this proposed agreement, CASO will implement a cloud-based document management and contract lifecycle management solution to modernize the Department's document storage, retrieval, workflow automation, and contract administration processes. Services include document scanning, electronic document management, contract lifecycle management, system configuration, user training, data migration, software maintenance, and technical support.

In accordance with Chapter 5, Section 511 of the Kern County Administrative Policy and Procedures Manual regarding the procurement of professional services, the Department conducted a competitive Request for Proposal (RFP) process for Comprehensive Software Solutions for Document Scanning, Electronic Document Management, and Contract Lifecycle Management in Fiscal Year 2026-2027. Following evaluation of proposals and completion of contract negotiations, CASO Document Management, Inc. was selected as the vendor whose proposal best met the Department's operational, technical, and business requirements. This agreement is the first year of a five-year RFP process. The next RFP for Comprehensive Software Solutions for Document Scanning, Electronic Document Management, and Contract Lifecycle Management is due in Fiscal Year 2031-2032.

This agreement has been approved as to form by the Office of County Counsel.

Therefore, IT IS RECOMMENDED that the Board approve the agreement with CASO Document Management, Inc. to provide comprehensive software solutions for document scanning, electronic document management, and contract lifecycle management for the period September 1, 2026, through August 31, 2031, in an amount not to exceed \$2,000,000, and authorize the Chairman to sign.

Respectfully submitted,



Alison Burrowes, MA, LCSW
Director

cc: County Administrative Office
County Counsel
Auditor-Controller-County Clerk

Kern County Agreement No. _____

**AGREEMENT FOR PROFESSIONAL SERVICES
(COUNTY OF KERN –CASO DOCUMENT MANAGEMENT,
INC.)**

**COMPREHENSIVE SOFTWARE SOLUTIONS FOR
DOCUMENT SCANNING, ELECTRONIC DOCUMENT
MANAGEMENT, AND CONTRACT LIFE CYCLE
MANAGEMENT**

FY 2026 – 2031

AGREEMENT FOR PROFESSIONAL SERVICES

(COUNTY OF KERN – CASO DOCUMENT MANAGEMENT, INC)

COMPREHENSIVE SOFTWARE SOLUTIONS FOR DOCUMENT SCANNING, ELECTRONIC DOCUMENT MANAGEMENT, AND CONTRACT LIFE CYCLE MANAGEMENT

THIS AGREEMENT is made and entered into on _____, by and between the County of Kern (“County”), a political subdivision of the State of California, as represented by the Behavioral Health and Recovery Services Department (“County”, “BHRS” or “Department”), and **CASO Document Management Inc, (“Contractor,” or “CASO”), a For Profit Corporation, with its principal place of business located at 134 West 29th Street, 11th Floor, New York, NY, 10001.**

WITNESSETH:

WHEREAS:

A. BHRS is implementing an electronic document management and contract lifecycle management program to digitize historical records, migrate electronic content, automate administrative workflows, improve records access, and strengthen information security and compliance.

B. CASO Document Management, Inc. will provide document scanning, data migration, EasyFile configuration and implementation, workflow and contract lifecycle management functionality, system integrations, training, technical support, and ongoing platform maintenance. CASO is also responsible for maintaining required privacy, cybersecurity, and records-handling safeguards. CASO’s services are limited to document conversion, migration, and electronic document management platform configuration and do not include interaction with BHRS clients or entry of data into the BHRS Electronic Health Record (EHR).

C. BHRS will provide oversight, define business requirements, participate in system design and testing, approve configurations and deliverables, coordinate access to records, facilities, systems, and staff, and authorize implementation and go-live. BHRS will retain ownership and control of its records and data and will remain responsible for ongoing day-forward scanning and system administration.

NOW, THEREFORE, IT IS AGREED between the parties hereto as follows:

1. TERM

This agreement shall commence on September 1, 2026, and shall remain in effect through August 31, 2031, unless sooner terminated as hereinafter provided.

2. MODIFICATIONS TO Agreement

This agreement may be modified only by a written amendment signed by both parties.

3. STANDARDS OF SERVICE

A. Contractor shall provide the services and adhere to the standards of service described in **Exhibit A, Description and Standards of Services**, which is attached hereto and made a part hereof. Failure to materially comply with the standards of service, which Contractor does not cure within thirty (30) days of written notice (or such shorter period as this Agreement specifies for the particular obligation), shall be deemed a material breach of this agreement and may result in termination of the agreement.

4. COMPENSATION TO CONTRACTOR

A. County shall reimburse Contractor for services provided and costs incurred in the provision of services in accordance with **Exhibit A, Description and Standards of Services**, up to the maximum amount set forth in **Exhibit C, Funding Schedule** which is attached hereto and made a part hereof.

B. No funds paid to Contractor through this Agreement shall be utilized to compensate employees of the Contractor for overtime or compensatory time off, except to the extent that Contractor is required to pay for overtime or compensatory time off, pursuant to the [Fair Labor Standards Act of 1938](#), [29 United States Code \(USC\) Section 201](#), et seq., or applicable state law.

C. This Agreement is subject to County's annual appropriation process. In the event that funds representing Contractor's compensation and reimbursement for expenses of the services provided pursuant to this Agreement are not appropriated within the approved County budget in any fiscal year, this Agreement shall be deemed terminated and shall be of no further force or effect as of the date County's budget is approved. County will provide Contractor with thirty (30) days' prior notice of any such action.

D. No payment shall be made to Contractor if Contractor has any federal, state, or county liens outstanding. Should County discover a record of an outstanding lien, County shall immediately notify Contractor about the lien record, immediately investigate the circumstances, and determine a course of action within thirty (30) days of discovery. The Department may consider a repayment arrangement between Contractor and the lien-maker as reasonably satisfying this Agreement stipulation. Contractor shall provide to County, within fifteen (15) days of request, a copy of the repayment arrangement document(s), the name of the contact person with the lien-maker agency that can verify the repayment arrangement, and a written statement explaining what resources Contractor is using to accomplish the repayment.

E. County will periodically evaluate Contractor's project costs for the purpose of assessing the reasonableness of County's payments for services provided. Contractor will be provided reasonable notice if additional contractual and/or service delivery issues are to be reviewed. Contractor is expected to prepare necessary reports and other material to adequately explain Contractor's use of funds as specified in **Exhibit C** of this Agreement. County may prescribe specific report formats and data content as deemed necessary at the sole discretion of County.

5. FINANCIAL SOLVENCY

Contractor shall maintain adequate provisions against the risk of insolvency.

6. TAX INFORMATION REPORTING

A. CASO Document Management, Inc. shall submit its signed IRS form W-9, "Request for Taxpayer Identification Number and Certification," or Social Security Number, whichever is applicable, to facilitate

appropriate fiscal management and reporting, and to ensure compensation is paid to the proper party. A new W-9 will need to be completed every five (5) years.

7. COMPLIANCE WITH LAW.

Each Party and any subcontractors will observe and comply with all applicable County, State, and federal laws, ordinances, rules, and regulations now in effect or hereafter enacted, each of which are made a part hereof and incorporated herein by reference.

8. NOTICES

A. All notices required or provided for in this agreement shall be provided to the parties at the following addresses, by personal delivery or deposit in the U.S. Mail, postage prepaid, registered or certified mail, addressed as specified below. Notices delivered personally shall be deemed received upon receipt; mailed or expressed notices shall be deemed received five (5) business days after deposit. A party may change the address to which notice is to be given by giving notice as provided below.

1. To County:

Behavioral Health and Recovery Services
Attn: Director
PO Box 1000
Bakersfield, CA 93302-1000
cc: Contracts Management

2. To Contractor:

CASO Document Management, Inc.
Richard Tamaro
134 West 29th Street, 11th Floor
New York, NY 10001
Richard.tamaro@caso.com

B. County requires Contractor to notify County thirty (30) days prior to any change in name, legal business status, corporate address, service site address, or Contractor's signatory power that occurs during the term of this agreement. At its option, County may choose to acknowledge a notice of these specific changes without a written amendment to the agreement.

C. Nothing in this Agreement shall be construed to prevent or render ineffective delivery of notices required or permitted under this agreement by personal service.

9. HIPAA/HITECH COMPLIANCE

A. During the term of this Agreement, Contractor may receive from BHRS, or may receive or create on behalf of BHRS, certain confidential health or Medi-Cal information ("Protected Health Information" or "PHI"). This PHI is subject to protection under state and federal law, including the [Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 \("HIPAA"\)](#), the [Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 \("the HITECH Act"\)](#), and regulations promulgated thereunder by the [U.S. Department of Health and Human Services](#) (the "HIPAA Regulations") and other applicable laws. CASO represents that it has in place policies and procedures that will adequately safeguard any PHI it receives or creates, and CASO specifically agrees, on behalf

of itself, its subcontractors, and agents, to safeguard and protect the confidentiality of PHI consistent with applicable law, including currently effective provisions of HIPAA, the HITECH Act, and the HIPAA Regulations.

B. For purposes of this section, PHI means any information, whether oral or recorded in any form or medium: (a) that relates to the past, present, or future physical or mental health condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual, and (b) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

C. The parties acknowledge that state and federal laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Agreement may be required to provide for procedures to ensure compliance with such developments. The parties hereto specifically agree to take such action as is necessary to implement the requirements of HIPAA, the HITECH Act, and HIPAA Regulations and other applicable laws relating to the security or confidentiality of PHI. The parties understand and agree that CASO must provide to BHRS, after request by BHRS, written evidence that CASO is in compliance with the HITECH Act and applicable HIPAA Regulations.

D. Notwithstanding any other provision of this Agreement, BHRS may terminate this Agreement upon twenty (20) days' notice in the event: (a) CASO does not promptly provide written evidence of compliance with the HITECH Act and applicable HIPAA Regulations, or (b) BHRS becomes aware that CASO or any of its subcontractors or agents discloses PHI in a manner that is not authorized by BHRS or by applicable law.

10. CONFIDENTIALITY.

Both Parties will not, without the written consent of the other party, communicate confidential information, designated in writing or identified in this Agreement as such, to any third party and shall protect such information from inadvertent disclosure to any third party in the same manner that it protects its own confidential information, unless such disclosure is required in response to a validly issued subpoena or other process of law. Upon completion of this Agreement, the provisions of this paragraph shall continue to survive.

11. MUTUAL INDEMNIFICATION.

All parties shall indemnify against any claim, demands, or liability arising from damage to property, and injuries to persons, which may arise out of or because of the Parties performance of its duties under this Agreement, or failure to perform, but only in proportion to and to the extent such claim demands, damages or liability are caused by, or result from the negligent or intentional acts or omissions of All Parties, its officers agent, or employees.

12. INSURANCE

Contractor, in order to protect County and its board members, officials, agents, officers, and employees against all claims and liability for death, injury, loss, and damage as a result of Contractor's actions in connection with the performance of Contractor's obligations, as required in this agreement, shall secure and maintain insurance as described below. Contractor shall not perform any work under this agreement until Contractor has obtained all insurance required under this section, and the required certificates of insurance and all required endorsements have been filed with the Department's Contracts Division. Receipt of evidence of insurance that does not comply with all applicable insurance requirements shall not constitute a waiver of the insurance requirements set forth herein.

The required documents must be signed by the authorized representative of the insurance company shown on the certificate. Upon request, Contractor shall supply proof that such person is an authorized representative thereof and is authorized to bind the named underwriter(s) and their company to the coverage, limits and termination provisions shown thereon.

Contractor shall promptly deliver to the Department's Contracts Division certificates of insurance, and all required endorsements, with respect to each renewal policy, as necessary to demonstrate the maintenance of the required insurance coverage for the term specified herein. Such certificates and endorsements shall be delivered to Department's Contracts Division prior to the expiration date of any policy and bear a notation evidencing payment of the premium thereof if so requested. Contractor shall immediately pay any deductibles and self-insured retentions under all required insurance policies upon the submission of any claim by Contractor or County as an additional insured.

A. Workers' Compensation and Employers Liability Insurance Requirements:

In the event Contractor has employees or volunteers who may perform any services pursuant to this agreement, Contractor shall submit written proof that Contractor is insured against liability for workers' compensation in accordance with the provisions of section 3700 of the California Labor Code.

Contractor shall require any subcontractors to provide workers' compensation for all of the subcontractors' employees, unless the subcontractors' employees are covered by the insurance afforded by Contractor. If any class of employees engaged in work or services performed under this agreement is not covered by California Labor Code section 3700, Contractor shall provide and/or require each subcontractor to provide adequate insurance for the coverage of employees not otherwise covered.

Contractor shall also maintain employer's liability insurance with limits of **ONE MILLION DOLLARS (\$1,000,000)** for bodily injury or disease.

B. Liability Insurance Requirements:

Contractor shall maintain in full force and effect, at all times during the term of this agreement, the following insurance:

a. Commercial General Liability Insurance including, but not limited to, Contractual Liability Insurance (specifically concerning the indemnity provisions of this agreement with the county), Products-Completed Operations Hazard, Personal Injury (including bodily injury and death), and Property Damage for liability arising out of Contractor's performance of work under this agreement. The Commercial General Liability insurance shall contain no exclusions or limitation for independent contractors working on the behalf of the named insured. Contractor shall maintain the Products-Completed Operations Hazard coverage for the longest period allowed by law following termination of this agreement. The amount of said insurance coverage required by this agreement shall be the policy limits, which shall be at least **ONE MILLION DOLLARS (\$1,000,000) each occurrence and TWO MILLION DOLLARS (\$2,000,000) aggregate.**

b. Automobile Liability Insurance against claims of Personal Injury (including bodily injury and death) and Property Damage covering any vehicle and/or all owned, leased, hired and non-owned vehicles used in the performance of services pursuant to this agreement with coverage equal to the policy limits, which shall be at least **ONE MILLION DOLLARS (\$1,000,000) each occurrence.**

c. Professional Liability (Errors and Omissions) Insurance, for liability arising out of, or in connection with, the performance of all required services under this agreement, with coverage equal to the policy limits, which shall not be less than **ONE MILLION DOLLARS (\$1,000,000) per occurrence and THREE MILLION DOLLARS (\$3,000,000) aggregate**.

d. Cyber Liability Insurance/Technology Professional Liability Insurance, for liability arising out of, or in connection with, the performance of all required services under this Agreement, involving access to personal and or confidential information, software or technology services where a data breach or exposure to personal and or confidential information could impact the County, coverage shall be equal to the policy limits, which shall be at least **ONE MILLION DOLLARS (\$1,000,000) per occurrence and TWO MILLION DOLLARS (\$2,000,000) aggregate**. Coverage shall respond to the duties and obligations as is undertaken by Contractor in this agreement and shall include, but not limited to, claims involving security breach, system failure, data recovery, business interruption, cyber extortion, social engineering, infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, and alteration of electronic information. The policy shall provide coverage for breach response costs, regulatory fines and penalties as well as credit monitoring expenses.

The Commercial General Liability insurance required in this sub-paragraph B shall include an endorsement naming County and County's board members, officials, officers, agents and employees as additional insureds for liability arising out of this agreement and any operations related thereto. Said endorsement shall be provided using one of the following three options: (i) on Insurance Services Office (ISO) form Commercial General (CG) 20 10 11 85; or (ii) on ISO form CG 20 37 10 01 plus either ISO form CG 20 10 10 01 or CG 20 33 10 01; or (iii) on such other forms which provide coverage at least equal to or better than form CG 20 10 11 85.

C. Any self-insured retentions in excess of **ONE HUNDRED THOUSAND DOLLARS (\$100,000)** must be declared on the Certificate of Insurance or other documentation provided to county and must be approved by the County Risk Manager.

D. If any of the insurance coverages required under this agreement is written on a claims-made basis, Contractor, at Contractor's option, shall either (i) maintain said coverage for at least three (3) years following the termination of this agreement with coverage extending back to the effective date of this agreement; (ii) purchase an extended reporting period of not less than three (3) years following the termination of this agreement; or (iii) acquire a full prior acts provision on any renewal or replacement policy.

E. Cancellation of Insurance – The above-stated insurance coverages required to be maintained by Contractor shall be maintained until the completion of all of Contractor's obligations under this agreement except as otherwise indicated herein. Each insurance policy supplied by the Contractor must be endorsed to provide that the coverage shall not be suspended, voided, canceled or reduced in coverage or in limits except after ten (10) days written notice in the case of non-payment of premiums, or thirty (30) days written notice in all other cases. Such notice shall be by certified mail, return receipt requested. This notice requirement does not waive the insurance requirements stated herein. Contractor shall immediately obtain replacement coverage for any insurance policy that is terminated, canceled, non-renewed, or whose policy limits have been exhausted or upon insolvency of the insurer that issued the policy.

F. All insurance shall be issued by a company or companies admitted to do business in the State of California and listed in the current “Best’s Key Rating Guide” publication with a minimum rating of A-; VII. Any exception to these requirements must be approved by the County’s Risk Manager.

G. If Contractor is, or becomes during the term of this agreement, self-insured or a member of a self-insurance pool, Contractor shall provide coverage equivalent to the insurance coverages and endorsements required above. County will not accept such coverage unless County determines, in its sole discretion and by written acceptance, that the coverage proposed to be provided by Contractor is equivalent to the above-required coverages.

H. All insurance afforded by Contractor pursuant to this agreement shall be primary to and not contributing to all insurance or self-insurance maintained by County. An endorsement shall be provided on all policies, except professional liability/errors and omissions, which shall waive any right of recovery (waiver of subrogation) against the county.

I. Insurance coverages in the minimum amounts set forth herein shall not be construed to relieve Contractor for any liability, whether within, outside, or in excess of such coverage, and regardless of solvency or insolvency of the insurer that issues the coverage; nor shall it preclude County from taking such other actions as are available to it under any other provision of this agreement or otherwise in law.

J. Failure by Contractor to maintain all such insurance in effect at all times required by this agreement shall be a material breach of this agreement by Contractor. County, at its sole option, may terminate this agreement and obtain damages from Contractor resulting from said breach. Alternatively, County may purchase such required insurance coverage, and without further notice to Contractor, County shall deduct from sums due to Contractor any premiums and associated costs advanced or paid by County for such insurance. If the balance of monies obligated to Contractor pursuant to this agreement is insufficient to reimburse County for the premiums and any associated costs, Contractor agrees to reimburse County for the premiums and pay for all costs associated with the purchase of said insurance. Any failure by County to take this alternative action shall not relieve Contractor of its obligation to obtain and maintain the insurance coverages required by this agreement.

13. BEHAVIORAL HEALTH AND RECOVERY SERVICES (BHRS) INSURANCE

Behavioral Health and Recovery Services (BHRS) shall at its sole cost and expense, provide coverage for its employees, students, and authorized agents for activities conducted in connection with this Agreement by maintaining in full force and effect programs of insurance and/or self-insurance as follows:

A. Workers’ Compensation and Employers Liability Insurance Requirements

In the event BHRS has employees or volunteers who may perform any services pursuant to this Agreement , BHRS shall submit written proof that BHRS is insured against liability for workers’ compensation in accordance with the provisions of section 3700 of the California Labor Code

B. Commercial General Liability Insurance

BHRS shall maintain in full force and effect, at all times during the term of this Agreement, the following insurance limits: **ONE MILLION DOLLARS (\$1,000,000) each occurrence and TWO MILLION DOLLARS (\$2,000,000) aggregate.**

C. Automobile Liability Insurance

BHRS shall maintain in full force and effect, at all times during the term of this Agreement the following insurance limits: **ONE MILLION DOLLARS (\$1,000,000)** each occurrence.

D. Professional Liability (Errors and Omissions) Insurance:

BHRS shall maintain in full force and effect, at all times during the term of this Agreement , the following insurance limits: **ONE MILLION DOLLARS (\$1,000,000) per occurrence and THREE MILLION DOLLARS (\$3,000,000)** aggregate.

F. Failure to maintain all such insurance in effect at all times required by this Agreement shall be a material breach of this Agreement.

14. NON-DISCRIMINATION AND FAITHFUL PERFORMANCE

A. The parties mutually agree to abide by all federal, state, and local laws including, but not limited to, all laws respecting employment discrimination. Each party further agrees to fully and faithfully perform all covenants and portions of this Agreement, and to take no action that may be inimical to the other party's faithful performance hereof.

15. REPRESENTATIONS

CASO makes the following representations, which are agreed to be material to and form a part of the inducement of this Agreement:

A. CASO has the expertise, training, and experience necessary to provide the services described in this Agreement; and

B. CASO does not have any actual or potential interest adverse to BHRS nor does Contractor represent a person or firm with an interest adverse to BHRS with reference to the subject of this Agreement; and

C. CASO is willing and able to diligently provide all required services in a timely and professional manner in accordance with the terms and conditions stated in this Agreement .

16. POLITICAL-RELIGIOUS ACTIVITY

A. No person performing any service or providing any goods designated under this Contract shall participate in any political or religious activity on County time or in any manner involving the use of county property or expenditure of public funds nor conveying the implication of County endorsement or support for a candidate for local, state, or federal office.

B. Notwithstanding the foregoing, nothing in this Contract shall be construed to unlawfully limit an individual's Constitutional rights. Accordingly, the limitations contained in this section are for the sole purpose of preventing proselytizing and politicking while engaged in the performance of services under this Contract.

17. NON-ASSIGNMENT AND SUBCONTRACTING

A. CASO shall not assign, sublet, or transfer this Agreement, or any part hereof, nor assign any monies due or that become due to CASO under this Agreement, without the prior written or electronic and express approval of County.

18. NO THIRD-PARTY BENEFICIARIES.

It is expressly understood and agreed that the enforcement of these terms and conditions and all rights of action relating to such enforcement, will be strictly reserved to both Parties. Nothing contained in this Agreement will give or allow any claim or right of action whatsoever by any other third person. It is the express intention of both Parties that any such person or entity, other than the Parties to this Agreement, receiving services or benefits under this Agreement will be deemed an incidental beneficiary only.

19. AUTHORITY TO BIND COUNTY

It is understood that CASO, in CASO's performance of any and all duties under this Agreement, except as otherwise provided in this Agreement, has no authority to bind County to any agreements or undertakings.

20. DISPUTE AND ISSUE RESOLUTION

A. Should a dispute occur concerning CASO's performance or CASO's interpretation of specific terms of this Agreement, CASO shall notify the KernBHRS Administrator of this issue within sixty (60) days of its occurrence. Such notification shall include specific identification of the issue(s) under dispute, CASO's factual basis for the issue, CASO's proposed solutions, and the documentary support for the solutions.

21. CHOICE OF LAW/VENUE

The parties hereto agree that the provisions of this Agreement will be construed pursuant to the laws of the state of California. This Agreement has been entered into and is to be performed in the County of Kern. Accordingly, the parties agree that the venue of any action relating to this Agreement shall be in the County of Kern.

22. NON-WAIVER

No covenant or condition of this Agreement can be waived except by the written consent of BHRS and CASO. Forbearance or indulgence by BHRS or CASO in any regard whatsoever shall not constitute a waiver of the covenant or condition to be performed by either Party. BHRS or CASO shall be entitled to invoke any remedy available to BHRS or CASO under this Agreement or by law or in equity despite said forbearance or indulgence.

23. ENFORCEMENT OF REMEDIES

No right or remedy herein conferred upon or reserved to BHRS or CASO is exclusive of any other right or remedy herein or by law or equity provided or permitted, but each shall be cumulative of every other right, or remedy given hereunder, now or hereafter existing by law or in equity or by statute or otherwise and may be enforced concurrently or from time to time.

24. CAPTIONS AND INTERPRETATION

A. Paragraph headings in this Agreement are used solely for convenience and shall be wholly disregarded in the construction of this Agreement.

B. No provision of this Agreement shall be interpreted for or against a party because that party or its legal representative drafted such provision, and this Agreement shall be construed as if jointly prepared by the parties.

25. TIME OF ESSENCE.

Time is hereby expressly declared to be of the essence of this Agreement and of each and every provision hereof, and each such provision is hereby made and declared to be a material, necessary and essential part of this Agreement.

26. COUNTERPARTS.

This Agreement may be executed simultaneously in any number of counterparts, each of which shall be deemed an original but all of which together shall constitute one and the same instruments.

27. NON-COLLUSION COVENANT.

CASO represents and agrees that it has in no way entered into any contingent fee arrangement with any firm or person concerning the obtaining of this Agreement with BHRS. CASO has not received from BHRS any incentive or special payments, or considerations not related to the provision of services under this Agreement.

28. ENTIRE AGREEMENT.

This document, including all attachments hereto, contains the entire Agreement between the parties relating to the services, rights, obligations and covenants contained herein and assumed by the parties respectively. No inducements, representations or promises have been made, other than those recited in this Agreement. No oral promise, modification, change or inducement shall be effective or given any force or effect.

29. NEGATION OF PARTNERSHIP.

In the performance of all services under this Agreement, CASO shall be, and acknowledges that CASO is, in fact and law, an independent contractor and not an agent or employee of BHRS. CASO has and retains the right to exercise full supervision and control of the manner and methods of providing services to BHRS under this Agreement. CASO retains full supervision and control over the employment, direction, compensation and discharge of all persons assisting CASO in the provision of services under this Agreement. With respect to CASO's employees, if any, CASO shall be solely responsible for payment of wages, benefits and other compensation, compliance with all occupational safety, welfare and civil rights laws, tax withholding and payment of employee taxes, whether federal, state or local, and compliance with any and all other laws regulating employment.

30. SEVERABILITY.

Should any part, term, portion or provision of this Agreement be decided finally to be in conflict with any law of the United States or the state of California, or otherwise be unenforceable or ineffectual, the validity of the remaining parts, terms, portions, or provisions shall be deemed severable and shall not be affected thereby, provided such remaining portions or provisions can be construed in substance to constitute the Agreement which the parties intended to enter into in the first instance.

31. TERMINATION.

Either party may terminate this Agreement, with or without cause, upon thirty (30) days prior written notice to the other party. In the event of termination of this Agreement for any reason, both Parties will have no further obligation to pay for any services rendered or expenses incurred by the other Party after the effective date of the termination.

32. IMMEDIATE TERMINATION.

Notwithstanding the foregoing, both Parties will have the right to terminate this Agreement effective immediately after giving written notice to the other Party in the event either Party determines that the other Party does not have the proper credentials, experience, or skill to perform the required services under this Agreement; or in the event that continuation by either Party in the providing of services may result (i) in civil, criminal, or monetary penalties against that Party, (ii) in the breach of any federal or state or regulatory rule or regulation or condition of accreditation or certification, or (iii) the loss or threatened loss of that Party's ability to participate in any federal or state program.

33. EXCLUSION REPORTING

a. CASO shall not knowingly have a relationship with any individual or entity that is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participating in any of such programs by any federal agency or by any department, agency or political subdivision of the state.

b. CASO must confirm the identity and determine the exclusion status of all employees and any subcontractor, as well as any person with an ownership or control interest, or who is an agent or managing employee through routine checks of federal and state databases.

c. [List of Excluded Individuals/Entities \(LEIE\)](#), which is maintained by the [United States Department of Health and Human Services \(HHS\)](#), [Officer of the Inspector General \(OIG\)](#), is updated upon hire and monthly thereafter.

d. This list includes entities and individuals who have been suspended from receiving payments for services.

e. If CASO or subcontractor is listed, this agreement shall terminate consistent with the paragraph entitled, "**IMMEDIATE TERMINATION.**" CASO shall ensure that any excluded individual is immediately prevented from performing services

f. The excluded individual should also be removed from active duty in any position in which the person's salary or the services rendered or prescribed are paid in whole or in part, by federal health care programs or federal funds until such time the person is removed from the Exclusions lists. Contractor shall maintain records confirming verification of initial and monthly monitoring for a minimum of ten (10) years after the employee's separation from employment.

g. CASO shall provide affirmation of review to the System of Care Administrator monthly, the Quality Improvement Division designee during annual audits and upon request, and shall, as prescribed by Department, report any provider individual, employee or subcontractor provider, appearing on any of these exclusions lists, databases or indices.

h. CASO must conduct an initial check, prior to hire new staff, of the following databases:

1. Social Security Administration's Death Master File, which is maintained by the United States Social Security Administration.
 2. [National Plan and Provider Enumeration System \(NPPES\)](#), which is maintained by the Centers for Medicaid and Medicare.
 3. [List of Excluded Individuals/Entities \(LEIE\)](#).
 4. [System for Award Management Excluded Parties List System \(SAM-EPLS\)](#).
 5. [Department of Health Care Services \(DHCS\) Medi-Cal Suspended and Ineligible Provider List \(S&I List\)](#)
- i. CASO must conduct monthly checks of the following databases:
1. [List of Excluded Individuals/Entities \(LEIE\)](#).
 2. [System for Award Management Excluded Parties List System \(SAM-EPLS\)](#).
 3. Department of Health Care Services (DHCS) Medi-Cal Suspended and Ineligible Provider List (S&I List)

34. DISCLOSURE OF OWNERSHIP AND CONTROL INTEREST STATEMENT

A. CASO agrees to furnish County with the names of its officers, owners, stockholders owning more than five percent (5%) of its stock, and major creditors holding more than five percent (5%) of the debt of CASO. This information shall become public record on file with the U.S. Department of Health and Human Services.

B. CASO agrees to comply with the requirements set forth in the federal regulations [42 CFR 455.104-455.106](#) in reference to the Medicare, Medicaid, or [Title XX service programs](#).

C. CASO agrees to submit to County the completed form attached herein as **Exhibit G, "Disclosure of Ownership and Control Interest Statement"** upon submitting the provider application, during the re-validation of enrollment, and upon request. Any person with a five percent (5%) or more direct or indirect interest in CASO must include results of fingerprints/criminal background check.

D. CASO agrees to notify County and update **"Disclosure of Ownership and Control Interest Statement"** within thirty-five (35) days if a change in ownership occurs.

E. County may terminate the Agreement if any person with a five percent (5%) or greater direct or indirect ownership interest in CASO does not submit timely and accurate information and cooperate with any screening methods required in [42 CFR 455.416](#).

35. REQUIRED DOCUMENTS

A. Agreements That Are Renewed Annually: Contractor shall submit all required documents to the Contract Monitoring Unit before BHRS sends the contract to the Board of Supervisors or County Purchasing Manager to be executed. Required documents include but are not limited to: Pre-Award Risk Assessment, Disclosure of Ownership Form.

B. Multi-Year Agreements: Contractor shall submit all required documents to the Contract Monitoring Team on or before or before March 1 annually. Failure to submit the required documents in a timely manner shall be deemed a material breach of this Agreement and may result in termination of the Agreement.

36. SIGNATURE AUTHORITY.

Each Party represents that they have full power and authority to enter into and perform this Agreement, and the person signing this Agreement on behalf of each Party has been properly authorized and empowered to enter into this Agreement.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK.]

IN WITNESS TO WHICH, each party to this agreement has signed this agreement upon the date indicated, and agrees for itself, its employees, officers, partners, and successors, to be fully bound by all terms and conditions of this agreement.

APPROVED AS TO CONTENT:

Behavioral Health and Recovery Services

COUNTY OF KERN

Board of Supervisors

By: Alison Burrowes
Alison Burrowes, MA, LCSW Director

By: _____
Chairman

APPROVED AS TO FORM:

Office of the County Counsel

CASO Document Management, Inc

By: Kyle W. Holmes
Kyle Holmes, Deputy

By: Richard Tamaro
Richard Tamaro

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

CASO DOCUMENT MANAGEMENT, INC

DOCUMENT MANAGEMENT COMPREHENSIVE SOFTWARE SOLUTIONS FOR DOCUMENT SCANNING, ELECTRONIC DOCUMENT MANAGEMENT, AND CONTRACT LIFE CYCLE MANAGEMENT

EXHIBIT A – DESCRIPTION AND STANDARDS OF SERVICES

1. PURPOSE AND PROJECT OBJECTIVES

The purpose of this project is to implement a unified, enterprise-level solution that addresses Kern Behavioral Health & Recovery Services' (Kern BHRS) critical needs for digitizing legacy paper records, managing ongoing employee and financial documentation, and enabling complete lifecycle management of contracts. The solution will modernize departmental operations, reduce physical storage costs, enhance document accessibility, and ensure compliance with regulatory standards governing protected health information and contractual records.

The primary objectives of this initiative are:

- **Digitization and Accessibility:**
Convert legacy medical records, historical employee files, and financial documents into searchable electronic formats, enabling rapid retrieval and secure access across all divisions.
- **Lifecycle Management:**
Provide robust contract lifecycle management capabilities, including automated template generation, version control, approval workflows, renewal notifications, and centralized repository for executed contracts.
- **Workflow Automation:**
Streamline contract and financial approval processes, automate routing and notifications, and support scalable electronic workflows with role-based access controls.
- **Compliance and Audit Readiness:**
Strengthen compliance with HIPAA, HITECH, DHCS, and 42 CFR Part 2 requirements through secure handling of protected health information, comprehensive audit logging, and robust data encryption.
- **Integration and Expansion:**
Leverage API integrations to create seamless workflows between existing systems, support future expansion of document volumes and workflows, and ensure compatibility with Kern BHRS business and work environments.
- **Operational Efficiency:**
Reduce physical storage costs and space requirements, improve document accessibility, and provide automated alerts for missing documentation, compliance deadlines, and critical timeline management activities.

2. ORDER OF PRECEDENCE AND VENDOR-SPECIFIC TERMS

The services in this Exhibit A incorporate the mandatory requirements of the documents identified in Source Documents below. In the event of a conflict, approved amendments, the executed Agreement and Exhibits, accepted portions of Vendor's proposal, the RFP addenda, and the RFP shall control in that order, unless the Agreement states otherwise.

3. ASSIGNED PERSONNEL

The following personnel are assigned to this engagement. Every team member with access to Kern BHRS records will complete current HIPAA training and comply with all applicable privacy and security requirements before beginning work.

Name	Role
Richard Tamaro	President & CEO / Project Sponsor
Bill Cross	Technical Lead EasyFile Architect
Michael Drew	EVP, Azure/Security Lead, Compliance Lead
Adam Fisk	Project Manager
Candice Vance	Project Manager (Southwest/California)
Daniel Shore	Senior Developer Integration Lead
Michael Kidder	Senior Developer / VP Technology Migration Lead
Aric Malsbury	Scanning Operations Lead Trainer

Contractor may substitute assigned personnel with individuals of equivalent qualifications and experience, subject to County approval, which shall not be unreasonably withheld or delayed.

Subcontractors / Consultants

No subcontractors are proposed for software platform delivery or scanning operations (outside the Temp Agency for the scanning team). Contractor may engage a HIPAA-compliant courier service for transport of physical records between Kern BHRS facilities and Contractor scanning operations where applicable. Any courier engaged will meet all HIPAA and 42 CFR Part 2 transport requirements specified in this RFP, including secure chain-of-custody controls and breach notification protocols. Contractor remains fully responsible for all subcontractor compliance.

4. PHASED IMPLEMENTATION PRIORITIES

Unless otherwise authorized in writing by Kern BHRS, the Contractor shall conduct implementation in phases and adhere to the division-priority order set forth herein.

1. Closed Medical Records
2. Contracts / Contract Lifecycle Management
3. Finance
4. Human Resources
5. Crisis Services
6. Medical Services
7. Correctional Behavioral Health

5. EASYFILE DISCOVERY, DESIGN, AND CONFIGURATION

Methodology – EasyFile Platform Delivery

Contractor's EasyFile delivery follows a structured, phase-driven methodology organized into five tracks that run in coordinated sequence across the engagement. Every track begins with

discovery — contractor to configure to Kern BHRS's actual processes, not generic templates — and end with a tested, trained, and accepted system that Kern BHRS staff operate independently.

Discovery and Requirements Validation

Discovery is the foundation of every EasyFile deployment and should not be skipped or abbreviated. For Kern BHRS, discovery is especially critical because this is the department's first enterprise document management implementation — there are no prior index structures, no existing workflows to replicate, and no established access-control policies to inherit. Everything must be designed collaboratively.

Discovery session structure (per division):

- Two to four hours with division subject matter experts (SMEs) and department leadership.
- Agenda: current document types and volumes, current storage and retrieval workflow, access control requirements, key metadata fields for search and reporting, workflow touchpoints, retention requirements, integration dependencies.
- Output: Division Requirements Summary document delivered within five business days of each session, reviewed and approved by Kern BHRS before configuration begins.

Discovery outputs used directly in configuration:

- Cabinet architecture map — cabinet names, sub-cabinet structure, document types per cabinet
- Metadata schema — all index fields, field types, validation rules, and lookup lists per document type
- Role and permission matrix — which user roles access which cabinets and document types
- Workflow specification — approval chain design, conditional logic, notification triggers, escalation timers
- Retention schedule — retention rules per document type, event-driven triggers, disposition approval requirements
- Integration specification — data fields, API endpoints, event triggers for each connected system

Platform Deployment and Core Configuration

EasyFile is provisioned on Microsoft Azure and configured to Kern BHRS's environment before any division goes live.

Environment provisioning (target: within 2 weeks of contract execution):

- Contractor provisions a dedicated EasyFile tenant on Microsoft Azure in a US-based data center.
- Azure environment configured with HIPAA-compliant controls: encryption at rest (AES-256), encryption in transit (TLS 1.2+), audit logging, access controls.
- Two environments deployed: Production and User Acceptance Testing (UAT). All configuration and testing occurs in UAT before promotion to Production.
- Microsoft Entra ID SSO via OIDC configured against Kern BHRS's existing Entra ID tenant. Users authenticate with existing County credentials.
- MFA enforced through the Entra ID identity provider.
- System health monitoring and alerting activated.

Division-by-Division Configuration and Go-Live

Each division follows the same four-step configuration cycle: Design → Build → Test → Go-Live. Divisions are configured sequentially per priority, with each go-live building on the stable foundation of all prior phases.

Step	Responsible Party	Activities
Design	Contractor & Kern BHRS	Cabinet architecture, metadata schema, workflow routing, role/permission matrix approved by Kern BHRS.
Build	Contractor	UAT cabinets, metadata fields, workflow rules, alert triggers, integration connections, redaction permissions, retention rules, Power BI data connector.
Test	Contractor & Kern BHRS	Contractor internal system testing. Kern BHRS SMEs perform UAT. Integration testing. Redaction tested by designated officers. All defects resolved before go-live approval.
Go-Live	Contractor & Kern BHRS	UAT sign-off. Configuration promoted to Production. Training delivered. Users provisioned. Contractor provides two-week hypercare period.

EasyFile Contract Lifecycle Management (CLM) Configuration (Phase 2 — Contracts Division)

Contractor's CLM is delivered on EasyFile Workflow — the full workflow engine — The following activities are specific to CLM and are in addition to standard division configuration:

CLM discovery activities (2–3 sessions with Contracts Division):

- Inventory of existing contract types and boilerplate language (basis for template library).
- Assessment of the existing internally-developed Contract Monitoring Tool (ASP.NET/SQL). Determine what functionality EasyFile CLM will replace or must integrate with via REST API.
- Map all approval chains: who approves which contract types, in what sequence or parallel arrangement, at what value thresholds.
- Define alert rules: renewal advance-notice days, expenditure-limit thresholds, stage-transition notifications, breach and termination triggers.
- Identify board letter template requirements.
- Define vendor and counterparty metadata structure.
- Map Power BI dashboard requirements: team view, requestor view, executive KPI view, financial/budget variance view.

CLM build deliverables:

- Smart Forms / eForms contract template library — each contract type selectable at creation, pre-populated with standard fields and boilerplate, with authorized customization. Board letter templates included.
- ECMTtoolbox Workflow approval workflow configurations: parallel and sequential routing per contract type, conditional logic, escalation timers.

- Full alert rule set via ECMToolbox Workflow: stage-entry notifications, deadline-missed alerts, renewal warnings, expenditure-limit alerts, procurement-readiness signals, termination and breach notifications.
- Skills-based task auto-routing and assignment — delivered as a product-level feature of ECMToolbox Workflow, available by Phase 2 go-live. Tasks automatically distributed based on subject-matter expertise and current workload.
- DocuSign Listener integration: real-time webhook with HMAC-SHA256 validation. Executed contracts automatically routed into the correct EasyFile cabinet.
- Dashboards: team pipeline view, requestor status view, executive KPI dashboard, lifecycle metrics, vendor compliance view, financial tracking and budget variance. Custom-built for Kern BHRS's specific operational needs.
- Work queue configuration: centralized task queue, routing rules by contract type and division, task assignment, workload visibility.
- Contract Monitoring Tool assessment and disposition decision (replace or integrate via REST API) made before build begins.

6. DIGITAL CONTENT MIGRATION

Kern BHRS has significant digital content stored across Microsoft SharePoint, Microsoft Teams, OneDrive, and network shares. Contractor migrates this content into EasyFile in phase sequence, concurrent with or immediately following each division's configuration.

- Medical Services Division: Authorization team documents on Share Drive (~477 GB).
- Correctional Behavioral Health: All documentation already in electronic format (~416 GB).
- Crisis Services: Digital content from Teams, SharePoint, and network shares (volume TBD).
- All divisions: SharePoint libraries, Teams document channels, and network share content per discovery inventory.

7. EASYFILE TRAINING DELIVERY

Contractor to deliver structured training to every Kern BHRS division before that division goes live. Training follows a train-the-trainer model supplemented by role-specific end-user sessions and supported by permanent self-service resources.

- Train-the-Trainer (2 days, per phase): Contractor trains designated Kern BHRS trainers.
- End-User Training (2–4 hours, role-based, in groups of 10–20): Contractor delivers division-specific end-user training.
- Administrator Training (1 full day, at system launch).
- CLM Power User Training (half-day, Contracts Division).
- Materials: role-specific user guides, administrator reference guide, quick-reference cards, knowledge base, release notes, annual refresher training.

8. PERFORMANCE STANDARDS, BENCHMARKS AND QUALITY ASSURANCE

System Performance Standards

Standard	Target	Measurement / Accountability
EasyFile Platform Uptime	99.9% monthly	Monthly uptime report to Kern BHRS account manager.
Search Response Time	Under 3 seconds	Platform health monitoring; included in monthly report.
Document Retrieval	Under 3 seconds from search result	Performance monitoring scope.

Standard	Target	Measurement / Accountability
Workflow Notification Delivery	Within 5 minutes of trigger	Workflow audit log.
API Response Time	Under 500ms for standard queries	Monitored. Baseline established during implementation.
Backup RPO	24 hours (daily snapshots)	Defined in service agreement. Annual DR test.
Backup RTO	4 business hours for critical system restoration	Defined in service agreement.

Support Response SLAs

Priority	Definition	Response Time	Resolution Target
P1 — Critical	System unavailable	2 business hours	Same business day or escalation plan
P2 — Major	Core feature impaired	4 business hours	Next business day
P3 — Standard	Non-critical issue or question	Next business day	Within 5 business days
P4 — Enhancement	Feature request	5 business days	Scheduled in next release or change order

Invoice Automation Benchmark (Finance Division, Phase 3)

Kern BHRS expects 90–95% of invoices and clinical forms to flow automatically from capture through indexing, approval routing, and filing with zero human touch. EasyFile Capture AI-powered indexing combined with the Workflow automated routing engine is designed to meet this benchmark. The 90–95% automation rate will be established as a formal performance benchmark in the Finance Phase 3 go-live acceptance criteria, measured over the first 30 days of production operation.

9. SECURITY CLEARANCE AND INFORMATION TECHNOLOGY REQUIREMENTS

Personnel Security Requirements

- Contractor personnel will undergo thorough background checks prior to assignment (criminal history, employment verification, references).
- All Contractor personnel with Kern BHRS records access must complete current HIPAA training before beginning work.
- Contractor will identify its Privacy Officer, Security Officer, and Compliance Officer to Kern BHRS within 30 days of contract award.
- Need-to-know access model: personnel access only systems and data required for their project role.
- Personnel changes affecting Kern BHRS access will be communicated to Kern BHRS within 24 hours; access to be revoked on same day of departure.

System Security Architecture

Security Domain	EasyFile Implementation
Hosting Infrastructure	Microsoft Azure (US data centers). FedRAMP High Authorization, SOC 1/2/3, ISO 27001, ISO 27017/27018.
CASO SOC 2 Type II	Security and Availability trust service criteria. Audit period: July 1, 2024 – June 30, 2025. Report available under NDA.
Identity and Access	Microsoft Entra ID SSO via OIDC. MFA enforced. Role-based access controls govern all cabinet, document-type, and function permissions.
Encryption	Data at rest: AES-256. Data in transit: TLS 1.2 minimum. API: OAuth2, JWT, API key authentication.
Audit Logging	All user activity logged with tamper-evident trail. Deletion requires authorized role and is permanently logged.
Redaction	Permanent data-level redaction via Apyrse WebViewer SDK. Redacted content destroyed at the data level — not masked. Original unredacted document preserved in permission-locked copy.
Backup and DR	Managed automated daily backups. RPO: 24 hours. RTO: 4 business hours. Periodic DR tests with documented results.
Incident Response	Documented procedure covering detection, containment, notification, documentation, recovery. Kern BHRS notified within 24 hours of confirmed breach.
42 CFR Part 2 (QSOA)	Contractor executes QSOA at contract award. All SUD record access governed by QSOA obligations in addition to HIPAA.
FOIA Compliance	Dedicated FOIA tracking: designated cabinet, deadline tracking, redaction workflow, audit trail of all FOIA-related actions.
AI Feature Security	All AI features (AI Connector, Capture AI, OCR) documented in Contractor's TAC AI Subcommittee review package. All features able to be disabled per cabinet or globally.

Kern County TAC Security Review

- County Administrative Policy Chapter 7, Section 719 requires cloud solutions not independently FedRAMP-certified to undergo formal security review by Kern County ITS Security and TAC.
- Contractor initiates TAC documentation package within 10 business days of contract execution.
- Package includes: SOC 2 Type II report, Azure FedRAMP documentation, EasyFile security architecture, data flow diagrams, AI feature disclosure, access control documentation, incident response procedures, data residency confirmation.
- Michael Drew leads TAC engagement; commits to responding to TAC requests within 5 business days.
- EasyFile can operate in limited configuration during TAC review with AI features activated upon TAC approval.

10. UTILIZATION OF COUNTY BUSINESS AND WORK ENVIRONMENT

Contractor's EasyFile delivery is designed to integrate into Kern BHRS's existing technology environment rather than displace it. County-provided assets will be incorporated directly into the EasyFile solution:

Microsoft Entra ID (Azure AD)	Identity provider for EasyFile SSO. No additional identity infrastructure required.
Microsoft Exchange Online / Office 365	EasyFile Mailbox Downloader via Microsoft Graph API. EFCconnector for in-Outlook filing. Native Office 365 application integration.
Microsoft Power BI (Government License)	EasyFile data feeds existing Power BI workspace for all CLM and operational dashboards. No additional BI licensing required.
DocuSign	EasyFile DocuSign Listener integrates with existing DocuSign account. No new DocuSign licensing.
Nintex K2	EasyFile REST API available for K2 integration. Scope defined during Phase 2 discovery.
Kern BHRS HRIS (ASP.NET Blazor / SQL)	EasyFile REST API enables integration once Kern BHRS ITS builds REST endpoints. Contractor provides full API documentation at Phase 4 kickoff.
AuditorNet / Workday (Kern 360)	EasyFile REST API designed and documented for future ERP integration.

Contractor does not require Kern BHRS to replace any existing system as a precondition of EasyFile deployment. Every connected system above is integrated, not replaced.

Day-forward scanning hardware: Contractor will recommend appropriate scanner models and quantities per division during the discovery phase. Kern BHRS may procure recommended models through existing purchasing channels or Contractor can source on their behalf — to be determined at project kickoff.

11. KERN BHRS RESPONSIBILITIES

Contractor's fixed pricing and the milestone dates stated in this Exhibit depend on the County actions described below, consistent with the County responsibilities identified in Recital C of this Agreement. Kern BHRS shall:

- A. Designate, and maintain for the duration of the implementation, a Project Sponsor, an Information Technology lead, division subject matter experts for each phase, an individual authorized to accept deliverables on behalf of Kern BHRS, and two (2) EasyFile administrators.
- B. Create the Microsoft Entra ID application registration required for EasyFile single sign-on.
- C. Provide DocuSign administrative access and register the DocuSign Listener webhook.
- D. Provide the contract types, boilerplate language, approval chains, value thresholds, and alert parameters required for the Contract Lifecycle Management build.
- E. Provide access to migration source systems, including SharePoint, Microsoft Teams, OneDrive, and network shares, together with an inventory of the content to be migrated.
- F. Provide access to the Kern BHRS-developed Chart Tracker system and, where applicable, the Kern BHRS SQL database, for evaluation as index auto-population sources.

- G. Ensure division subject matter expert participation in discovery sessions and in user acceptance testing for each phase.
- H. Provide the workspace, power, high-speed internet access, facility access, and daily coordination contact described in the section of this Exhibit entitled On-Site Scanning.
- I. Make the day-forward scanning hardware procurement decision described in this Exhibit at project kickoff.
- J. Review and approve, or provide written comment on, Division Requirements Summaries and other deliverables submitted by Contractor for County approval.

Review and approval periods. Unless this Agreement specifies a different period for a particular item, Kern BHRS shall provide approval, written comment, or written notice of deficiency within ten (10) business days of Contractor's submission.

Effect of delay. Where Kern BHRS does not perform a responsibility stated in this Section within the applicable period, and Contractor's performance is delayed as a direct result, the affected Contractor milestone dates stated in this Exhibit shall extend day-for-day. This paragraph shall not apply to the June 12, 2027 completion date for Closed Medical Records, which Contractor treats as a firm commitment notwithstanding any such delay.

12.ADDITIONAL OPTIONS AND ENHANCEMENTS

Additional options and system enhancements may be made available to Kern BHRS upon request. These items are not included in the base proposal pricing and will be offered with clearly identified associated costs. Any such additional options or enhancements shall only be incorporated into the Agreement through a written amendment, executed by both parties.

Option A – AI Connector Deployment Model

EasyFile's AI Connector can be deployed in two models. BYOK is recommended for Kern BHRS given the sensitivity of behavioral health data.

Model	Description	Cost
BYOK (Bring Your Own Key)	Kern BHRS provides its own Anthropic API key. Data flows to Anthropic under Kern BHRS's direct agreement.	Anthropic API usage billed directly to Kern BHRS at Anthropic's published rates. No Contractor surcharge.
Contractor-Managed	Contractor provides Anthropic API access under Contractor's account.	Usage billed through Contractor at cost + 15% administration fee.

Option B – Extended Support Hours

Option	Details and Pricing
Base Support (Included)	M–F 8:00 AM – 6:00 PM Pacific. P1: 2hr; P2: 4hr; P3: next business day.
Extended Hours — Evenings	To 10:00 PM Pacific M–F. +\$6,000/year.
Extended Hours — Weekend	Saturday 9:00 AM – 5:00 PM Pacific. +\$8,000/year.
24/7 Emergency Coverage	P1 emergency response 24/7/365. +\$15,000/year.

Option C – Additional Power BI Dashboard Development

Base proposal includes standard CLM and operational dashboards. Custom dashboards beyond the standard set:

Service	Rate
Custom Power BI Dashboard Development	\$2,500 per dashboard (design, build, Kern BHRS review, two revision cycles)
Power BI Training	\$1,500 per half-day session

13. WORK SCHEDULE AND TRANSITION PLAN

August 31, 2026 Commitment

Contractor will begin pre-implementation activities within 5 business days of receiving a notice of intent to award. Site survey, team mobilization, Azure environment provisioning, and Entra ID SSO planning will all be underway before August 31, 2026 — meeting the RFP's project start requirement regardless of contract execution timing.

Master Milestone Schedule — EasyFile Platform

Milestone	Target Date	Responsible Party
Notice of intent to award — pre-implementation activities begin	Immediately upon notice	Contractor
Project kickoff meeting	Within 5 days of contract execution	Contractor & Kern BHRS
EasyFile UAT + Production environments provisioned on Azure	September 15, 2026	Contractor
Entra ID SSO integration live (UAT)	September 15, 2026	Contractor & Kern BHRS
TAC security documentation package submitted	Within 10 business days of contract execution	Contractor
Phase 1 CMR cabinet structure configured (UAT)	September 30, 2026	Contractor
Closed Medical Records searchable in EasyFile — rolling	October 1, 2026 onward	Contractor
Phase 2 CLM discovery sessions complete	October 31, 2026	Contractor & Kern BHRS
Contract Monitoring Tool assessment complete.	November 15, 2026	Contractor & Kern BHRS
CLM Smart Forms template library built (UAT)	December 15, 2026	Contractor
CLM approval workflows and alert rules configured	December 31, 2026	Contractor
DocuSign Listener integration live (UAT)	January 15, 2027	Contractor
CLM Power BI dashboards built	January 31, 2027	Contractor
Contracts Division go-live (Phase 2)	February 1, 2027	Contractor & Kern BHRS

Milestone	Target Date	Responsible Party
Phase 3 Finance discovery sessions complete	February 28, 2027	Contractor & Kern BHRS
AP workflow configured (UAT)	March 15, 2027	Contractor
Finance Division go-live (Phase 3)	April 1, 2027	Contractor & Kern BHRS
Phase 4 HR discovery sessions complete	May 31, 2027	Contractor & Kern BHRS
HR Division go-live (Phase 4)	July 1, 2027	Contractor & Kern BHRS
Crisis Services go-live (Phase 5)	October 1, 2027	Contractor & Kern BHRS
Medical Services + CBH digital migration complete	December 15, 2027	Contractor
Full deployment go-live (Phase 6)	January 1, 2028	Contractor & Kern BHRS
Year 1 account review	February 2028	Contractor & Kern BHRS

The milestone dates and target timelines stated in Exhibit A, including the Master Milestone Schedule and any related phase or division targets, are planning estimates only. Dates may be adjusted, in whole or in part, to align with County department needs, operational readiness, staffing availability, or workflow dependencies, upon mutual written acknowledgment between Contractor and Kern BHRS (e-mail is sufficient). Such adjustments shall not, by themselves, constitute a breach of this Agreement, provided Contractor maintains overall progress and complies with any expressly identified hard deadlines, including the Closed Medical Records hard deadline of June 12, 2027.

14. SOFTWARE, COMPUTER TECHNOLOGY, AND LICENSE AGREEMENTS

Component	Vendor/ Technology	License / Delivery
EasyFile EDM	Contractor	SaaS subscription. Included in 5-year EasyFile Automation subscription.
EasyFileX Web Client	Contractor (Blazor/.NET)	Included. Browser-based, no installation.
EFDesktop	Contractor (.NET Windows)	Included. Windows installer.
EasyFile Capture	Contractor	Included.
ECMToolbox Workflow / Smart Forms (CLM Engine)	Contractor	Included. Configuration delivered as Phase 2 professional service.
EasyFile Mailbox Downloader	Contractor / Microsoft Graph API	Included.

Component	Vendor/ Technology	License / Delivery
EFConnector (Outlook)	Contractor / Microsoft Office Add-in	Included.
EasyFile REST API	Contractor	Included. Full documentation, code samples, SDKs.
EasyFile AI Connector	Contractor / Anthropic Claude API	Included in platform. AI usage charges per Anthropic rates (BYOK) or Contractor-managed pricing.
Apryse WebViewer SDK (Viewer, Redaction, OCR)	Apryse	Licensed by Contractor. Embedded in EasyFile. No separate license.
Microsoft Azure (Hosting)	Microsoft	Contractor's Azure subscription. Included.
Microsoft Entra ID	Microsoft	Kern BHRS's existing tenant. No additional licensing.
DocuSign	DocuSign	Kern BHRS's existing account.
Microsoft Power BI	Microsoft	Kern BHRS's existing government license.

Kern BHRS will execute the following agreements, each of which shall be incorporated into the Contract as additional Exhibits and executed concurrently with contract execution:

- EasyFile Subscription Agreement — Contractor's standard SaaS agreement.
- Business Associate Agreement (BAA) — HIPAA/HITECH.
- Qualified Service Organization Agreement (QSOA) — 42 CFR Part 2.
- Anthropic API Terms of Service (BYOK option only).

Kern BHRS is not required to execute separate license agreements with Microsoft (Azure, Entra ID, Power BI, Exchange), DocuSign, Apryse, or Fujitsu — these are the Contractor's vendor relationships embedded in the EasyFile subscription or Kern BHRS's existing agreements.

15. SCANNING SERVICES APPROACH

Contractor's scanning scope for Kern BHRS is built around a single principle Kern BHRS stated consistently throughout the RFP and both addenda:

- Historical backfile is scanned by Contractor. Ongoing, day-forward scanning is performed by Kern BHRS staff — Contractor operates no day-forward scanning service.

Accordingly, this section addresses the one-time conversion of Kern BHRS's historical paper records. Contractor will scan, index, OCR, quality-check, and deliver these records into EasyFile, and will return every physical document to Kern BHRS. Contractor performs no day-forward scanning of any kind; ongoing scanning across all divisions is Kern BHRS responsibility, supported by the hardware, EasyFile Capture automation, and training described above in this Exhibit.

Contractor's scanning scope comprises three confirmed historical backfile collections:

Priority	Collection	Volume	Forecasted Pages	Contractor Role
1	Closed Medical Records	~55,000 files	~2.75M–8.25M (est.)	Physical scanning — top priority, firm June 12, 2027 deadline
3	Finance Division Records	300 banker boxes	~600,000–750,000 (est.)	Physical scanning
4	Employee Records (historical/inactive)	140 banker boxes	~200,000–400,000 (est.)	Physical scanning

The priority numbers follow the division priority order stated in the section on Phased Implementation Priorities. Priority 2 (Contracts / Contract Lifecycle Management), Priority 5 (Crisis Services), and Priority 6 (Medical Services) are digital-migration divisions with no physical paper to scan. Refer to the documented Scope Clarifications (below) on Correctional Behavioral Health and the Psychiatric Evaluation Center.

Forecasted page and image volume (planning estimate)

Kern BHRS advised across the RFP and both addenda that page counts vary widely and that an average is generally not available. The figures below are Contractor planning estimates used to size crew, equipment, and schedule and are not a basis for pricing. Because Closed Medical Records are priced per file (with a small per-page increment for files over 100 pages) and Finance and Employee Records are priced per carton, Kern BHRS carries no page-count pricing risk: the price is fixed regardless of how the page counts resolve.

Collection	Basis (RFP / addenda)	Forecasted pages	Notes
Closed Medical Records	No usable average available; planning assumption of ~50–150 pages/file for behavioral-health closed charts.	2,750,000–8,250,000	Widest range; firmed by sampling and Chart Tracker.
Finance Division	No page average available (Addendum 2); only the 300-box count is firm. Planning factor of ~2,000–2,500 sheets per 15" box.	600,000–750,000	Box-based estimate only.
Employee Records	Addendum 2: most folders 70–200 pages, several 300–700; 8–14 folders per box. ~11 folders × 140 boxes ≈ 1,540 folders.	200,000 – 400,000 (likely 250,000–300,000)	Best-supported estimate of the three.

Forecast methodology and confirmation path

Image counts run modestly above the sheet counts above depending on the actual duplex rate, which Contractor confirms by sampling. The Closed Medical Records range is the widest because no per-file average exists anywhere in the RFP record; Contractor will narrow it two ways before crews mobilize: (1) a sampling exercise at the site survey, scheduled within five

days of notice of intent to award, and (2) metadata from the BHRS-developed Chart Tracker system where available. Contractor will model production throughput against multiple page-per-file scenarios at the site survey to confirm crew and equipment sizing against the firm June 12, 2027, deadline.

Note on digital volumes: the gigabyte figures referenced for several divisions in the RFP describe existing electronic content slated for migration into EasyFile — not paper to be physically scanned. They are addressed elsewhere in this exhibit and are not part of this scanning forecast.

16. ON-SITE SCANNING – CONTRACTOR’S PRIMARY APPROACH

Kern BHRS expressed a clear preference for on-site scanning to maintain an unbroken chain of custody over sensitive behavioral health records. Contractor has positioned on-site scanning as the primary approach for this engagement, and on-site execution is a core, consistent capability for Contractor — not an occasional accommodation.

Contractor will deploy a complete, self-contained production operation into the Kern BHRS Closed Medical Records facility in Bakersfield. Contractor brings its full production environment to the Kern BHRS's location: production scanners, workstations, server infrastructure when required, and Contractor's complete software stack, including EasyFile Capture. A structured team — project manager, on-site supervisor, scanning operators, and dedicated QC reviewers — manages every stage of production inside Kern BHRS's facility, with little to no burden on Kern BHRS's internal IT team.

Because scanning is performed on-premises, the records never leave Kern BHRS's control. Contractor's chain-of-custody documentation, two-layer quality control, and tracking logging apply on-site exactly as they do in Contractor's production facilities, and Kern BHRS staff have live access to records in EasyFile as they are scanned — searchable and reviewable from the first day of production, even while the team is working on-site.

Contractor requirements from Kern BHRS for On-Site Work

Kern BHRS will provide the following for on-site work:

- A dedicated workspace with adequate square footage for scanning equipment and document staging
- Power access for scanners and workstations
- High-speed internet access for delivery into EasyFile
- Facility access for Contractor staff during agreed production hours
- A designated Kern BHRS contact for daily coordination and issue escalation

Offsite Hybrid Flexibility

Should any portion of the work be more efficiently completed off-site, Contractor can transport records under HIPAA- and 42 CFR Part 2-compliant secure transport with real-time tracking and a manifest logged at departure and arrival. On-site remains the primary approach for this engagement; off-site is available only where Kern BHRS elects it and chain-of-custody requirements are fully satisfied.

On-Site staffing forecast – Closed Medical Records

Because no per-file page average exists for the 55,000 Closed Medical Records, Contractor has modeled the on-site crew needed to meet the firm June 12, 2027 deadline across three page- volume scenarios that bracket the forecast range. The scenarios let Kern BHRS see, in

advance, the on-site footprint each volume implies — and let both parties size the workspace, power, and schedule accordingly.

Planning Assumptions

A production window of approximately 193 working days (Closed Medical Records scanning begins September 2, 2026; completes June 12, 2027), a single 8-hour shift, and a planning throughput of roughly 12,500 pages per scanning station per day for prepped behavioral-health charts — i.e., each fully staffed station processes approximately 2.4 million pages over the engagement. These assumptions are calibrated by the site survey and the opening pilot batch before full production; prep intensity is the main variable and can shift the figures.

On-site resource	Scenario A 3M pages	Scenario B 5M pages	Scenario C 8M pages
Required daily throughput	~15,500 pages/day	~26,000 pages/day	~41,500 pages/day
Scanning stations	2	3	4
Scanner operators	2	3	4
Prep technicians	2	3	4
QC technicians	1	1	2
On-site supervisor	1	1	1
Total Contractor staff on-site	6	8	11
Shift pattern	Single shift	Single shift	Single shift

A dedicated Contractor project manager supports the engagement in addition to the on-site crew above and is covered by the Onsite Project Set-up and Management Fee (see Exhibit C).

17. SCOPE OF SCANNING SERVICES

Closed Medical Records – Priority 1

- Volume: Approximately 55,000 files. Per-file page counts are unavailable from Kern BHRS; Contractor prices this collection per file (with a small per-page increment for files over 100 pages), insulating Kern BHRS from page-count risk. Forecasted production volume ~2.75M–8.25M pages.
- Date range: 1961–2008
- Storage: Expandable file folders on shelves and 15" banker boxes
- Condition: Good. Documents held with prong fasteners; some staples; some double-sided pages possible. Predominantly 8.5×11", some 8.5×14" (legal) and smaller; nothing larger than 11×14" expected.
- **Hard deadline:** All 55,000 files scanned, indexed, uploaded, and verified by June 12, 2027, as Kern BHRS is vacating the storage facility. Contractor treats this as a firm operational commitment.

Turnaround commitments (firm):

- Batch turnaround: Every batch in Contractor's possession is returned within 7 calendar days of Contractor taking physical possession.

- Rush retrieval: Any individual file in the scanning queue is made available within 24 hours of a Kern BHRS records request, every day throughout the project.

Indexing fields:

- Medical record number
- Client first name
- Client last name
- Date of birth
- Additional fields to be confirmed during discovery with Closed Medical Records SMEs
- Contractor will evaluate the Kern BHRS-developed Chart Tracker system during discovery as a potential source for index auto-population.

Finance Division Records – Priority 3

- Volume: 300 banker boxes (15" standard)
- Content: Primarily contractor reimbursements organized by fiscal year, plus other financial documents
- Access sensitivity: Role-based access controls in EasyFile so Finance records are visible only to authorized Finance staff
- Indexing: No predefined index structure exists. Contractor will develop the index schema collaboratively with Finance Division SMEs during discovery. The schema will be designed to support a future Workday (Kern 360) synchronization without requiring it at go-live.
- Return: Records returned to boxes organized by fiscal year.

Human Resources – Employee Records (Historical / Inactive) – Priority 4

- Volume: 140 banker boxes (15" standard)
- Condition: Green legal hanging folders (8.5×14"); each folder contains six tabbed, fastener-bound sections; some staples. Most folders run 70–200 pages with several reaching 300–700, and boxes hold 8–14 folders each — approximately 1,540 folders across the 140 boxes, forecast at ~200,000–400,000 pages.
- Document-level indexing (six to seven sections per folder):
 - Employee Information
 - Medical
 - Confidential (direct deposit, W-4, I-9, beneficiary information)
 - EPRs (performance reviews)
 - Credentials
 - Livescan
 - Employee-Relations - (Some folders include an additional employee-relations section.)
- Privacy controls: The Medical and Confidential sections are flagged at indexing so EasyFile restricts access to HR administrators with appropriate permissions. General HR staff cannot view Confidential section contents.
- Integration: Contractor will evaluate the Kern BHRS SQL database for current employees during discovery as a potential source for historical metadata auto-population. Historical paper files without an electronic equivalent are captured through scanning.
- Return: Records returned to the correct six-section folder structure.

18. SCANNING DOCUMENT PREPARATION

Document preparation is performed by Contractor and is included in the all-inclusive per-file and per-carton rates (see Exhibit C) – there is no separate prep charge.

Collection	Preparation
Closed Medical Records	Remove files from expandable folders and banker boxes, remove prong fasteners, remove staples where encountered, unfold folded documents, scan, reassemble each file to its folder in original order (not re-stapled).
Finance Division	Open boxes, remove from folders, scan, return to boxes organized by fiscal year.
Employee Records	Remove from hanging folders, remove fasteners from each of the six sections, scan, reassemble to correct section order.

19. SCANNING TECHNICAL SPECIFICATIONS

Specification	Standard
Resolution	Minimum 300 DPI
Color mode	Color and black & white, per RFP
Duplex	Duplex scanning for all double-sided pages
Feed method	Auto-feed for standard pages; flatbed available for fragile or unusual formats
OCR	Applied to every image; full-text searchability required. Primarily typed text; some handwritten content present in closed medical records — advanced handwriting OCR applied where feasible.
Output formats	PDF/A (archival) and searchable PDF with embedded text layer; TIFF where required for production archives. Final format confirmed against EasyFile repository requirements during setup.
Page sizes	Primary 8.5×11"; also 8.5×14" (legal) and smaller; up to 11×14" handled if present.
Production equipment	Contractor deploys production scanners (auto-feed, duplex, letter through legal/11×14"), with flatbed capture for fragile or oversized items. Equipment is matched to material at the site survey. Day-forward hardware for Kern BHRS operated scanning is addressed elsewhere in this Exhibit A.
Indexing software	EasyFile Capture with AI-powered field extraction and automated indexing from structured layouts; human review for low-confidence extractions.

20. COMPLIANCE – HIPAA AND 42 CFR PART 2

This is a substance use disorder treatment records project. Closed medical records are protected under 42 CFR Part 2 in addition to HIPAA/HITECH. Contractor will satisfy every compliance prerequisite before handling a single record:

- **Business Associate Agreement (BAA)** – HIPAA/HITECH. Included as a separate Exhibit. Contractor executes as part of this agreement.

- **Qualified Service Organization Agreement (QSOA)** – 42 CFR Part 2. Contractor has confirmed it can execute the QSOA; a QSOA is required in addition to the BAA, and no SUD records are handled until it is in place. Contractor's compliance lead, Michael Drew, is responsible for execution.
- **HIPAA training** – All staff assigned to this project complete current HIPAA training; documentation is maintained on file and available to Kern BHRS on request.
- **Designated officers** – Contractor will provide Privacy Officer, Security Officer, and Compliance Officer contact information to Kern BHRS within 30 days of contract award.
- **HIPAA compliance program documentation** – Written policies, procedures, security practices, breach protocols, and audit-logging procedures provided to Kern BHRS.
- **Background checks** – All scanning staff undergo thorough background checks (criminal history, employment verification, references). Specific clearance requirements confirmed at contract execution.
- **Audit logging** – Access controls and audit trails enabled on all Contractor scanning systems used for this project; every access to a SUD record during scanning is logged (who, when, what).

42 CFR Part 2 Compliance Requirements:

Access to Substance Use Disorder (SUD) records is strictly limited to staff who have a documented need to perform their duties. All Contractor personnel who handle SUD records are subject to the obligations outlined in the Qualified Service Organization Agreement (QSOA). At no point are SUD records discussed with or disclosed to individuals who are not authorized to receive them.

Contractor's breach-notification procedures specifically include SUD records governed under the QSOA, extending beyond the obligations contained in the HIPAA Business Associate Agreement. Contractor also maintains documented procedures demonstrating how compliance with 42 CFR Part 2 is upheld throughout the entire records-handling lifecycle, including pre-scan activities, scanning, indexing, uploading, and final return of materials.

21. CHAIN OF CUSTODY AND QUALITY ASSURANCE

Chain of Custody

- A chain-of-custody manifest is created before any file leaves its original storage location, logging file identifier, date/time removed, the Contractor staff member, and destination.
- Files are tracked from removal through scanning through return; the return is documented with date, condition, and receiving staff.
- All physical documents are returned to Kern BHRS after scanning. There is no certified destruction of Kern BHRS records. Medical records are returned to their folders in correct order (not re-stapled); employee records to the correct six-section structure; finance records to boxes organized by fiscal year.
- For any off-site transport elected by Kern BHRS, Contractor uses a HIPAA-compliant courier under signed agreement, with real-time tracking, sealed and manifested containers opened only at a secure Contractor scanning environment, and files never left unattended in transit.

Quality Assurance

Every batch must pass Contractor's QC process before delivery and upload:

- Automated completeness check — every page in every file accounted for against the manifest.

- Image quality review — legibility, correct orientation, and confirmation that no pages were unintentionally dropped.
- OCR validation — text layer present and readable on sampled pages.
- Metadata validation — all required index fields populated; no blank required fields.
- Human QC sampling — minimum 10% of each batch reviewed by a QC technician independent of the scanning operator.
- Exception handling — pages failing QC are rescanned before delivery; pages that cannot be successfully digitized are flagged and reported to Kern BHRS with explanation.

Monthly Progress Reporting

Contractor provides Kern BHRS a monthly report covering volume processed, volume remaining, quality metrics (rescan rate, exception count), and schedule status against milestones.

22. ADDITIONAL SCANNING SCOPE CLARIFICATIONS

Crisis - Psychiatric Evaluation Center (PEC) – Priority 5

Non-EHR PEC documents (property logs, health assessments, and similar) enter EasyFile at roughly 400,000–500,000 images per year. This is an ongoing, day-forward volume and is Kern BHRS's responsibility, performed by Kern BHRS staff — it is not part of Contractor's scanning scope. EHR-bound clinical documents are scanned by Kern BHRS staff directly into SmartCare and are likewise out of scope. Contractor performs no day-forward scanning at PEC; the day-forward tooling and training that support Kern BHRS staff are addressed earlier in this Exhibit.

Correctional Behavioral Health (CBH) – Priority 7

There are no physical documents to be scanned and that CBH content (416 GB) already exists in electronic format to be imported into the EDM. Contractor treats CBH as digital migration into EasyFile — there is no physical scanning and no Contractor scanning crew. Any ongoing CBH documents are Kern BHRS's day-forward responsibility and are not part of Contractor's scanning scope.

23. SCANNING TIMELINE AND MILESTONES

Milestone	Target	Notes
Contract execution	August 2026	Target
Site survey — Closed Medical Records facility	Within 5 days of notice of intent to award	Before contract execution where possible
On-site scanning crew deployed	September 1, 2026	Within 14 days of contract execution
Closed Medical Records scanning begins	September 2, 2026	
50% of CMR files scanned and in EasyFile	January 29, 2027	Milestone payment trigger
100% of CMR files scanned and in EasyFile	June 12, 2027	Hard deadline — facility vacated

Milestone	Target	Notes
Finance Division scanning begins	April 2027	Phase 3 (Finance go-live Q2 2027)
Finance scanning complete	June 30, 2027	
Employee Records scanning begins	July 2027	Phase 4 (HR go-live Q3 2027)
Employee Records scanning complete	September 30, 2027	

All dates identified in the Scanning Timeline and Milestones table are targets intended for planning purposes and may be advanced or deferred to accommodate department priorities and workflow sequencing. Adjustments will be coordinated through the Kern BHRS Project Sponsor and recorded in the monthly progress report. Nothing in this paragraph modifies or waives any hard deadline expressly stated elsewhere in this Exhibit.

24. DATA OWNERSHIP AND END-OF-TERM SERVICES

Data Ownership

All Kern BHRS Data—including scanned images, metadata, indexes, extracted fields, audit logs, configuration files, and any derivative outputs—shall remain the sole and exclusive property of Kern Behavioral Health and Recovery Services. Contractor obtains no ownership interest and may use the data only as necessary to perform contracted services. No secondary use, monetization, AI-training, aggregation, or disclosure is permitted. Refer to the BAA, which is included in this agreement as a separate exhibit, for further information on data ownership.

Return of Data.

Upon Kern BHRS's request, expiration of the Agreement, or termination of the Services, Contractor shall promptly return Kern BHRS Data to Kern BHRS in a usable, structured, commonly readable format reasonably requested by Kern BHRS.

Secure Deletion.

After returning Kern BHRS Data, or upon Kern BHRS's written direction, Contractor shall securely delete all remaining Kern BHRS Data in Contractor's possession or control, except to the extent retention is required by law. Any retained Kern BHRS Data shall remain subject to this agreement and applicable exhibits until deleted.

Certification of Deletion.

Upon request, Contractor shall provide a written certification signed by an authorized representative confirming completion of deletion required by this Agreement.

Exit Assistance.

Contractor shall provide reasonable transition assistance, at the rates expressly stated in the Agreement or otherwise at mutually agreed rates if not already addressed, to facilitate migration of Kern BHRS Data and continuity of Services to Kern BHRS or a replacement provider.

25. ADDITIONAL INFORMATION

FedRAMP and Kern County TAC Security Review

EasyFile is hosted on Microsoft Azure, which holds FedRAMP High Authorization covering the cloud infrastructure layer. Contractor's application-layer security posture will be provided to the

Kern County ITS Security team and Technical Advisory Committee (TAC) for the formal security review required by County Administrative Policy Chapter 7, Section 719. Contractor will cooperate fully with the TAC review process and supply all documentation required.

AI Disclosure Summary

EasyFile includes AI/ML-powered components as disclosed in Section 5.4. Contractor will provide full AI feature disclosure documentation to the TAC AI Subcommittee as required, covering feature inventory, data handling, model governance, security controls, third-party dependencies (Anthropic API, Apyrse OCR), and administrative opt-out settings. All AI features can be disabled on a per-feature or per-cabinet basis by EasyFile administrators.

News Releases

Contractor agrees that no news releases pertaining to any award resulting from this RFP will be made without prior written approval of the Director of Kern Behavioral Health & Recovery Services.

Organizational Conflict of Interest

Contractor warrants, to the best of its knowledge, that neither Contractor nor its officers, agents, or employees presently has any consulting or contractual arrangement with any firm or organization that would give rise to an organizational conflict of interest with respect to the work to be performed under this agreement. Contractor will immediately notify Kern BHRS if any such conflict of interest is identified and will cooperate in presenting a suitable mitigation plan.

Time of Essence

Notwithstanding the foregoing, the milestone dates and target timelines stated in Exhibit A are planning estimates and may be adjusted to align with County department needs or workflow dependencies. Only deadlines expressly identified as “hard deadlines” in this Agreement (including the Closed Medical Records deadline of June 12, 2027) shall be treated as fixed dates to which time is of the essence applies.

26. SOURCE DOCUMENTS

This exhibit and Exhibit C were prepared from the County of Kern Request for Proposal to Provide Comprehensive Software Solutions for Document Scanning, Electronic Document Management, and Contract Lifecycle Management, issued April 28, 2026, Addenda Nos. 1 and 2, and the selected bidder's proposal.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

CASO DOCUMENT MANAGEMENT, INC

DOCUMENT MANAGEMENT COMPREHENSIVE SOFTWARE SOLUTIONS FOR DOCUMENT SCANNING, ELECTRONIC DOCUMENT MANAGEMENT, AND CONTRACT LIFE CYCLE MANAGEMENT

EXHIBIT B – ADDITIONAL ADMINISTRATIVE AND ETHICAL REQUIREMENTS

Contractor shall provide to County:

1. Mission: The organization's mission statement and related policies indicating Contractor's dedication to the same or similar mission as Kern Behavioral Health and Recovery Services. The statement or policies shall include a requirement that employees will be trained in and expected to uphold a code of ethical conduct.

2. Insurance: Certificates of adequate and appropriate insurance as required in the paragraph of this agreement entitled "**INSURANCE.**" A written description of the advisory body's or management's accountability process assuring Contractor maintains proper and adequate insurance.

3. Statutory Responsibilities: Documentation delineating Contractor's plan to monitor the following statutory responsibilities:

- A. Ensuring that all labor laws relating to individuals and employers are obeyed.
- B. Adherence to labor standards, human rights, and occupational health and safety regulations.
- C. Commitment to an anti-drug work environment.
- D. Enforcement of non-smoking regulations.
- E. Ensuring that all computer software copyright laws are enforced.

4. Fiscal: Written documentation in the form of plans, policies, and/or statements outlining and demonstrating their strategies for providing management of funds received from Kern Behavioral Health and Recovery Services. The statement shall demonstrate the following:

- A. Contractor's internal accounting control processes;
- B. The oversight responsibility of an advisory body or management's accountability process for financial matters. The strategy described may be unique to Contractor as long as it can clearly demonstrate oversight and accountability.

C. An organizational chart showing the relationship and major duties for financial management as distributed among an advisory body and/or chief executive officer and chief financial officer or other comparable positions.

5. Contracts: A statement or plan proving their awareness of organizational obligations regarding contracts, including the requirements and consequences for failure to meet funding source obligations, and a plan for monitoring the organization's compliance with contractual obligations.

6. Accreditation: In lieu of the requirements herein, Contractor shall provide to County documentation of accreditation from a County-recognized accreditation body, including but not limited, to CARF or the Joint Commission on Accreditation of Healthcare Organizations. Such accreditation warrants, and County concurs, that Contractor meets the requirements set forth in this Exhibit, provided Contractor continuously maintains valid accreditation during the term of this agreement. Contractor shall notify County within twenty-four (24) hours of any change in the status of its accreditation. Contractor agrees that County may ask for, and Contractor shall provide, information with regard to the items listed here.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

CASO DOCUMENT MANAGEMENT, INC

DOCUMENT MANAGEMENT COMPREHENSIVE SOFTWARE SOLUTIONS FOR DOCUMENT SCANNING, ELECTRONIC DOCUMENT MANAGEMENT, AND CONTRACT LIFE CYCLE MANAGEMENT

EXHIBIT C – FUNDING SCHEDULE – PRICING AND PAYMENT FOR SERVICES

SEPTEMBER 1, 2026 – AUGUST 31, 2031

1. SCANNING SERVICES

Pricing is structured around a fixed setup fee plus per-collection unit rates. All unit rates are all-inclusive: document preparation, HIPAA and 42 CFR Part 2 compliance, OCR, quality control, indexing, upload to EasyFile, transport, and return of physical documents. There is no separate document preparation charge — preparation is included in the unit rate, reflecting the operational reality that scanning these record types requires Contractor to perform the full prep cycle as part of the service.

Fixed Project Fee

This fee covers mobilization and demobilization of Contractor's on-site production environment, project management and on-site supervision for the scanning engagement, equipment delivery and removal, and compliance set-up (BAA and QSOA execution, staff background checks, HIPAA training, and onboarding). It is fixed and non-prorated — payable in full regardless of final volumes — and establishes the project's fixed-cost floor.

Item	Basis	Amount
Onsite Project Set-up and Management Fee	One-time, fixed	\$25,000

Per-Collection Rates

Collection	Unit	Rate
Closed Medical Records	Per file (first 100 pages)	\$15.00
Closed Medical Records	Per page over 100 pages in a file	\$0.10
Finance Division Records	Per carton	\$375.00
Employee Records	Per carton	\$375.00
Rush retrieval (24-hour individual file)	Per event	\$75.00

Estimated Scanning Total

Item	Quantity	Estimated
Onsite Set-up and Management Fee	1	\$25,000
Closed Medical Records (base, \$15.00/file)	55,000 files	\$825,000

Item	Quantity	Estimated
Closed Medical Records — page overage (>100 pages/file)	On actuals	Billed on actuals
Finance Division	300 cartons	\$112,500
Employee Records	140 cartons	\$52,500
Rush retrieval	On actuals	Billed on actuals
ESTIMATED SCANNING TOTAL (excluding actuals)		\$1,015,000

Closed Medical Records Page Overage

The \$15.00 per-file rate applies to every file and covers the first 100 pages. Pages beyond 100 within a single file are billed at \$0.10 each, on the actual page counts captured during scanning. Kern BHRS confirmed across multiple addenda responses that no per-file page average is available; the overage is therefore billed on actuals rather than estimated, and the flat \$15.00 base applies regardless of file thickness. This hybrid structure splits the page-count risk between both parties — Kern BHRS pays a flat rate for the large majority of files and only a modest per-page increment for unusually thick charts, while Contractor is not exposed to undercounting on multi-volume files.

Page Count Sampling and Adjustment Protocol

Contractor will conduct page-count sampling of approximately 200 Closed Medical Records files during the site survey, scheduled within five business days of notice of intent to award. Contractor will deliver a revised pricing forecast based on the sampled average within 10 business days of the survey. If the sampled average indicates total actuals will materially exceed the \$2,000,000 five-year budget ceiling, Contractor and Kern BHRS will negotiate adjustments to scope, ceiling, or rate structure before scanning operations begin.

2. EASYFILE PLATFORM — FIVE-YEAR SUBSCRIPTION

EasyFile Automation tier, 300 named users. All modules included: EasyFile EDM, ECMToolbox Workflow / Smart Forms (CLM), EasyFile Capture, EasyFile Mailbox Downloader, DocuSign Listener, AI Connector, REST API, and Microsoft Entra ID SSO. No per-module or per-feature fees. No CPI escalation for the contract term.

The first subscription year shall commence on the commencement date of the Term stated in Section 1 of this Agreement, and each subsequent subscription year shall commence on the anniversary of that date, such that five (5) subscription years fall within the Term.

Year 1	Year 2	Year 3	Year 4	Year 5	5-Year Total
\$80,000	\$80,000	\$80,000	\$80,000	\$80,000	\$400,000

3. PROFESSIONAL SERVICES (ONE-TIME, FIXED)

Professional Services are scoped against the full 18-month active implementation timeline (August 2026 through January 2028 go-live) plus initial post-go-live stabilization. Hours are estimated at a blended Contractor rate of \$250 per hour reflecting senior developers, project managers, implementation specialists, and trainers. All Professional Services are billed as one-time fixed amounts per milestone — no time-and-materials exposure for Kern BHRS.

Professional Services by Section Summary
Discovery & Requirements Validation (6 divisions × ~20 hrs each: sessions, prep, write-ups, sign-off cycles)
EasyFile System Configuration & Cabinet Architecture (6 divisions — cabinet structure, metadata schemas, role/permission matrix, RBAC)
EasyFile CLM Build — ECMToolbox Workflow + Smart Forms Template Library + Alert Rules (parallel/sequential routing, 7 alert types, Contract Monitoring Tool assessment, Power BI dashboards)
EasyFile Capture & Automation Build — AP invoice processing (90–95% straight-through target), check log automation, correspondence routing, HR 6-section auto-classification, CMR intake capture, Medical Services authorization workflow
Integration Work — Microsoft Entra ID SSO, DocuSign Listener (webhook + HMAC-SHA256), REST API specifications for HRIS, Power BI data connector, Microsoft Graph API for Mailbox Downloader, future Workday and K2 integration foundation
Digital Content Migration — ~900GB across 6 divisions: SharePoint, Teams, network shares, CBH (~416GB), Medical Services Share Drive (~477GB). Includes inventory, metadata mapping, migration execution, validation
Training Delivery — Train-the-Trainer (2 days × 6 phases), end-user training (role-based, division-specific), administrator training, CLM Power User training, Capture admin training
Project Management — 18-month active implementation engagement (~9 hours per month average), milestone tracking, client communications, risk management, cross-functional coordination
TOTAL PROFESSIONAL SERVICES - \$530,000

3.1 Professional Services Scope Assumptions

The Professional Services pricing above is fixed-fee based on the scope of work defined in Exhibit A. The following items, if they materialize during implementation, are scope additions and will be addressed through mutually executed amendment to the Agreement rather than absorbed into base pricing:

- Contract Monitoring Tool integration via EasyFile REST API (rather than full replacement by EasyFile CLM) — assessed in Phase 2 discovery and priced separately if integration is required.
- Workday (Kern 360) bi-directional integration — deferred pending County Auditor authorization; will be scoped and priced as an amendment when authorized.
- Capture AI model expansion beyond the workflows listed above (AP, check log, correspondence, HR sections, CMR intake, Medical Services authorization).
- Digital content migration significantly exceeding the ~900GB scoped above, or migration requiring substantial metadata cleanup or re-organization beyond standard bulk import with auto-generated metadata.
- Additional dashboards beyond the standard CLM and operational dashboards delivered in Phase 2 — available at \$2,500 per dashboard (see Additional Options and Enhancements in Exhibit A).
- Additional user licenses above the 300 named users in the base subscription.

3.2 Service Delivery Sites

Service delivery sites may include, but are not limited to, the locations listed below. Additional sites may be designated as necessary to meet project requirements.

- 2525 North Chester Avenue, Bakersfield, CA 93308
- 2001 28th Street, Bakersfield, CA 93301
- 820 34th Street, Bakersfield, CA 93301
- 1608 Norris Road, Bakersfield, CA 93308

4. CONTINGENCY FUNDING

A contingency funding allocation of \$55,000 is established under this Agreement. Contingency funds may be utilized by Kern BHRS, in whole or in part, to cover costs associated with any items designated as “billed on actuals” within this Agreement, including but not limited to additional professional services, configuration adjustments, incremental usage-based charges, and other scope elements that cannot be reasonably forecast at contract execution. Use of contingency funds shall not require a revision to base pricing; however, expenditures against the contingency amount must be documented and invoiced in accordance with the Agreement’s invoicing requirements.

Contingency funds may only be used up to the \$55,000 limit. Any need exceeding this amount shall require a mutually executed Amendment to the Agreement prior to incurring additional costs.

5. FIVE-YEAR FUNDING SUMMARY

Cost Category	Total
Scanning Services — Estimated (excluding actuals)	\$1,015,000
EasyFile Platform — 5-Year Subscription (fixed)	\$400,000
Professional Services (one-time, fixed)	\$530,000
Contingency Funding	\$55,000
AGREEMENT FUNDING TOTAL	\$2,000,000

6. ADDITIONAL PRICING NOTES

- All prices are fixed for the five-year contract term. No CPI escalation is applied to any line item.
- Scanning costs are billed at the stated unit rates as work is completed per the milestone payment schedule.
- The \$1,015,000 estimated scanning total excludes (a) page overage charges for Closed Medical Records files exceeding 100 pages, billed at \$0.10 per page on actuals, and (b) rush retrieval events at \$75 per event, billed as incurred. Actuals will be confirmed against the site survey sampling protocol described in Exhibit A and the Page Count Sampling and Adjustment Protocol stated above.
- Document preparation is included in all-inclusive per-file and per-carton scanning rates — no separate prep charge. Contractor has elected to include preparation in the base rate because the operational reality of scanning behavioral health charts, employee folders with fastener-

bound sections, and financial records with fiscal-year organization requires Contractor to perform the full preparation cycle as a standard part of the service. The all-inclusive pricing simplifies invoicing and eliminates ambiguity over what is and is not included.

- Day-forward scanning hardware is not included in this pricing. Contractor will recommend appropriate scanner models and quantities per division during the discovery phase. Kern BHRM may procure recommended models through existing purchasing channels or Contractor can source on their behalf — to be determined at project kickoff.
- Professional Services are scoped per the assumptions stated in this Exhibit. Scope additions are addressed through mutually executed amendment(s) to the Agreement.

7. PAYMENT AND INVOICING

A. Invoices generally. Contractor shall submit invoices to the Department's designated fiscal contact, accompanied by the Claim for Payment form attached as Exhibit I where required by County. Each invoice shall identify the agreement number, the billing period, the cost category (Scanning Services, EasyFile Subscription, Professional Services, or Contingency Funding), and the supporting detail described below. County shall pay all undisputed amounts within thirty (30) days of receipt of a complete invoice. If County disputes any portion of an invoice in good faith, County shall notify Contractor in writing within fifteen (15) days of receipt, identifying the disputed amount and the basis for the dispute, shall pay the undisputed balance when due, and the parties shall resolve the disputed portion in accordance with the dispute resolution provisions of this Agreement.

B. Scanning Services. The Onsite Project Set-up and Management Fee of \$25,000 shall be invoiced upon execution of this Agreement and is fixed and non-prorated. Contractor shall invoice Scanning Services every two (2) weeks in arrears, on actuals, at the per-collection unit rates stated in this Exhibit, for units completed during the billing period. For this purpose a "unit" means a Closed Medical Records file, or a Finance Division or Employee Records carton, that has been scanned, indexed, uploaded to EasyFile, and has passed Contractor's quality control process as described in Exhibit A. Each scanning invoice shall be accompanied by a production report for the billing period stating files and cartons completed, page counts in excess of one hundred (100) pages per Closed Medical Records file, and rush retrieval events, reconciled to the monthly progress report required by Exhibit A, such that each invoice is verifiable as units multiplied by the applicable contract rate.

C. Items billed on actuals. Notwithstanding the Contingency Funding provisions of this Exhibit, Closed Medical Records page overage at \$0.10 per page over one hundred (100) pages in a file, and rush retrieval events at \$75.00 per event, are payable at the stated contract rates as billed on actuals and shall not require an amendment to this Agreement or authorization against the Contingency Funding allocation, except to the extent that total compensation under this Agreement would exceed the Agreement Funding Total. Nothing in this paragraph limits the operation of the Page Count Sampling and Adjustment Protocol stated in this Exhibit.

D. Professional Services. Professional Services are fixed-fee and shall be invoiced upon completion and County acceptance of the following milestones, each of which corresponds to a milestone stated in Exhibit A:

Milestone	Amount
M1 — Contract execution and project kickoff meeting held	\$53,000
M2 — UAT and Production environments provisioned; Entra ID SSO live in UAT; TAC documentation package submitted	\$79,500
M3 — Phase 1 Closed Medical Records cabinet structure configured and accepted in UAT	\$53,000
M4 — CLM Smart Forms template library built in UAT; approval workflows and alert rules configured; Contract Monitoring Tool assessment delivered	\$53,000
M5 — Contracts Division go-live accepted (Phase 2), including DocuSign Listener integration and CLM dashboards	\$79,500
M6 — Finance Division go-live accepted (Phase 3), including AP workflow	\$79,500
M7 — Human Resources Division go-live accepted (Phase 4)	\$53,000
M8 — Crisis Services go-live accepted (Phase 5)	\$26,500
M9 — Full deployment go-live accepted (Phase 6) and implementation closeout	\$53,000
TOTAL PROFESSIONAL SERVICES	\$530,000

Acceptance of each milestone shall follow the user acceptance testing sign-off and go-live approval process described in Exhibit A. County shall provide acceptance, or a written statement of material deficiencies, within ten (10) business days of Contractor's written notice of delivery. Acceptance shall not be unreasonably withheld or delayed, and a milestone shall be deemed accepted if County provides neither acceptance nor a statement of material deficiencies within that period. Where a milestone is delayed by causes attributable to County or to third parties outside Contractor's control, the parties shall confer regarding invoicing for work completed.

For avoidance of doubt, the dates associated with Professional Services milestones are planning targets intended for scheduling and resource coordination. Invoicing shall occur upon County acceptance of a delivered milestone as set forth in Paragraph D, irrespective of any adjustment to target dates. Any schedule adjustments will be coordinated with the Kern BHRS Project Sponsor and reflected in the monthly progress report described in Exhibit A.

E. EasyFile Subscription. The annual subscription fee of \$80,000 shall be invoiced annually in advance, in accordance with the subscription year provisions stated in Section 2 of this Exhibit.

F. Contingency Funding. Amounts charged against the Contingency Funding allocation shall be separately identified on invoices, supported by the documentation described in this Exhibit, and applied against the \$55,000 limit. Contractor shall state the remaining Contingency Funding balance on each invoice that draws against it.

G. Agreement Funding Total. Total compensation under this Agreement shall not exceed the Agreement Funding Total of \$2,000,000 absent a mutually executed amendment. Contractor shall notify County in writing when cumulative invoiced amounts reach eighty-five percent (85%) of the Agreement Funding Total.

H. Expenses. All travel, lodging, per diem, equipment transport, and other expenses incurred by Contractor in performing this Agreement are included within the fixed Professional Services amounts and the all-inclusive Scanning Services unit rates stated in this Exhibit. Contractor shall submit no separate charge for expenses.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK.]

CASO DOCUMENT MANAGEMENT, INC

DOCUMENT MANAGEMENT COMPREHENSIVE SOFTWARE SOLUTIONS FOR DOCUMENT SCANNING, ELECTRONIC DOCUMENT MANAGEMENT, AND CONTRACT LIFE CYCLE MANAGEMENT

EXHIBIT D - BUSINESS ASSOCIATE ADDENDUM

THIS BUSINESS ASSOCIATE ADDENDUM ("Addendum") supplements and is made a part of the agreement ("agreement") by and between the County of Kern ("Covered Entity" or "CE") and **CASO Document Management, Inc.** ("Business Associate" or "BA"). This Addendum is effective as of date first written above (the "Addendum Effective Date").

RECITALS:

A. CE wishes to disclose certain information to BA pursuant to the terms of the agreement, some of which may constitute Protected Health Information ("PHI"), Personal Information ("PI"), or Personally Identifiable Information ("PII") (defined below). For the purpose of this Exhibit, PHI, PI, and PII all refer to confidential information that must be protected.

B. CE and BA intend to protect the privacy and provide for the security of PHI disclosed to BA pursuant to the agreement in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("the HITECH Act"), and regulations promulgated thereunder by the U.S. Department of Health and Human Services (the "HIPAA Regulations") and other applicable laws.

C. As part of the HIPAA Regulations, the Privacy Rule and the Security Rule (defined below) require CE to enter into a contract containing specific requirements with BA prior to the disclosure of PHI, as set forth in, but not limited to, [Title 45, Sections 164.314\(a\), 164.502\(e\), and 164.504\(e\)](#) of the Code of Federal Regulations ("CFR") and contained in this Addendum.

D. In consideration of the mutual promises below and the exchange of information pursuant to this Addendum, the parties agree as follows:

1. DEFINITIONS

A. Catch-All Definition: The following terms used in this agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

B. Specific Definitions:

1. 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 party to this agreement, shall mean **CASO Document Management, Inc.**

2. 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 the County of Kern.

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

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

5. Personal Information (PI) shall mean information that identifies or describes an individual, including, but not limited to, name, social security number, physical description, address, telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual.

6. Personally Identifiable Information (PII) means any information about an individual which can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, and biometric records. This information can be in paper or electronic files and includes, but is not limited to, education records, financial transactions, employment history, criminal records, and medical files.

7. Privacy Rule shall mean the HIPAA Regulation that is codified at [45 CFR Parts 160](#) and [164](#), Subparts A and E.

8. Protected Health Information (PHI) means individually identifiable health information that is transmitted or maintained in any form or medium, created or received by a health care provider or health plan, that relates to past, present, and future physical or mental health condition of an individual; provisions of healthcare to an individual; or past, present, and future payment for the provision of healthcare to an individual. Health information that is considered subject to the regulations contained in the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) includes: name, date of birth, telephone number, names of relatives, names of employers, photographic images, facsimile number, medical record number, finger or voice prints, certificate/license number, social security number, internet (IP) address, web URL, e-mail address, and any device or serial number. “Protected Health Information” includes electronic protected health information.

2. PERMITTED USES AND DISCLOSURES

A. BA may only use or disclose PHI, PI, or PII as necessary to perform the services set forth in the attached agreement.

B. BA may use or disclose PHI, PI, or PII as required by law.

C. BA agrees to make uses and disclosures and requests for PHI, PI, or PII consistent with CE's minimum necessary policies and procedures.

D. BA may not use or disclose PHI in a manner that would violate [Subpart E of 45 CFR Part 164](#) if done by CE except for the specific uses and disclosures set forth below.

E. BA may use PHI, PI, or PII for the proper management and administration of BA or to carry out the legal responsibilities of BA.

F. BA may disclose PHI, PI, or PII for the proper management and administration of BA or to carry out the legal responsibilities of BA, provided the disclosures are required by law, or BA obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was

disclosed to the person, and the person notifies BA of any instances of which it is aware in which the confidentiality of the information has been breached.

G. BA may provide data aggregation services relating to the health care operations of CE.

3. OBLIGATIONS AND ACTIVITIES OF BA

BA agrees to:

A. Use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic PHI to prevent use or disclosure of PHI other than as provided for by the agreement;

B. In accordance with [45 CFR 164.502\(e\)\(1\)\(ii\)](#) and [164.308\(b\)\(2\)](#), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of BA agree to the same restrictions, conditions, and requirements that apply to BA with respect to such information;

C. Make available PHI in a designated record set to CE as necessary to satisfy CE's obligations under [45 CFR 164.524](#);

D. Make any amendment(s) to PHI in a designated record set as directed or agreed to by CE pursuant to [45 CFR 164.526](#), or take other measures as necessary to satisfy CE's obligations under [45 CFR 164.526](#);

E. Maintain and make available the information required to provide an accounting of disclosures to CE as necessary to satisfy CE's obligations under [45 CFR 164.528](#);

F. Provide beneficiaries with the Notice of Privacy Practices, in accordance with [45 CFR 164.520](#) and BHRS Policy 10.1.21;

G. To the extent BA is to carry out one or more of CE's obligations under [Subpart E of 45 CFR Part 164](#), comply with the requirements of Subpart E that apply to CE in the performance of such obligation(s);

H. Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

I. Report to CE any use or disclosure of PHI, PI, or PII not provided for by the agreement of which it becomes aware, including breaches of unsecured PHI as required at [45 CFR 164.410](#), and any security incident of which it becomes aware, without unreasonable delay, and in no case later than one (1) business day of discovery [[42 USC Section 17921](#); [45 CFR Section 164.504\(e\)\(2\)\(ii\)\(C\)](#); [45 CFR Section 164.308\(b\)](#)].

Notwithstanding the foregoing, the parties acknowledge that unsuccessful Security Incidents occur routinely against systems connected to the internet, including without limitation pings and other broadcast attacks on BA's firewall, port scans, unsuccessful log-on attempts, denial-of-service attacks that do not result in the system being taken offline, and malware blocked before execution, in each case that do not result in unauthorized access, use, disclosure, modification, or destruction of PHI, PI, or PII. This paragraph constitutes notice of such unsuccessful Security Incidents, and BA shall report them in aggregate summary form upon CE's written request, no more frequently than quarterly. This paragraph applies to security-incident reporting under this agreement and all exhibits.

4. BA's Agents. BA shall ensure that any agents, including subcontractors, to whom it provides PHI, agree in writing to the same restrictions and conditions that apply to BA with respect to such PHI and implement the safeguards required by Paragraph A above with respect to Electronic PHI [[45 CFR Section 164.504\(e\)\(2\)\(ii\)\(D\)](#); [45 CFR Section 164.308\(b\)](#)]. BA shall implement and maintain sanctions against agents and subcontractors that violate such restrictions and conditions and shall mitigate the effects of any such violation (see [45 CFR Sections 164.530\(f\)](#) and [164.530\(e\)\(1\)](#)).

5. Amendment of PHI. If applicable, within ten (10) days of receipt of a request from CE for an amendment of PHI or a record about an individual contained in a Designated Record Set, BA or its agents or subcontractors shall make such PHI available to CE for amendment and incorporate any such amendment to enable CE to fulfill its obligations under the Privacy Rule, including, but not limited to, [45 CFR Section 164.526](#). If any individual requests an amendment of PHI directly from BA or its agents or subcontractors, BA must notify CE in writing within five (5) days of the request. Any approval or denial of amendment of PHI maintained by BA or its agents or subcontractors shall be the responsibility of CE [[45 CFR Section 164.504\(e\)\(2\)\(ii\)\(F\)](#)].

6. Accounting Rights. Within ten (10) days of notice by CE of a request for an accounting of disclosures of PHI, BA and its agents or subcontractors shall make available to CE the information required to provide an accounting of disclosures to enable CE to fulfill its obligations under the Privacy Rule, including, but not limited to, [45 CFR Section 164.528](#), and the HITECH Act, including but not limited to 42 USC Section 17935(c), as determined by CE.

A. BA agrees to implement a process that allows for an accounting to be collected and maintained by BA and its agents or subcontractors for at least six (6) years prior to the request, for all disclosures made without written consent. However, accounting of disclosures from an Electronic Health Record for treatment, payment, or health care operations purposes are required to be collected and maintained for only three (3) years prior to the request, and only to the extent that BA maintains an electronic health record and is subject to this requirement.

B. At a minimum, the information collected and maintained shall include: (i) the date of disclosure; (ii) the name of the entity or person who received PHI and, if known, the address of the entity or person; (iii) a brief description of PHI disclosed; and (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's authorization, or a copy of the written request for disclosure.

C. In the event that the request for an accounting is delivered directly to BA or its agents or subcontractors, BA shall within five (5) days of a request forward it to CE in writing. It shall be CE's responsibility to prepare and deliver any such accounting requested. BA shall not disclose any PHI except as set forth in this Addendum [[45 CFR Sections 164.504\(e\)\(2\)\(ii\)\(G\)](#) and [164.528](#)]. The provisions of this subparagraph shall survive the termination of this agreement.

7. Governmental Access to Records. BA shall make its internal practices, books, and records relating to the use and disclosure of PHI available to CE and to the Secretary of the U.S. Department of Health and Human Services (the "Secretary") for purposes of determining BA's compliance with the Privacy Rule [[45 CFR Section 164.504\(e\)\(2\)\(ii\)\(H\)](#)]. BA shall provide to CE a copy of any PHI that BA provides to the Secretary concurrently with providing such PHI to the Secretary.

8. Data Ownership. BA acknowledges that BA has no ownership rights with respect to the PHI.

9. BA shall report to covered entity any use or disclosure of PHI not provided for by the agreement of which it becomes aware, including breaches of unsecured PHI as required at [45 CFR 164.410](#), [45 CFR Section 164.504\(e\)\(2\)\(ii\)\(C\)](#) and [45 CFR Section 164.308\(b\)](#).

10. Notification of Breach. During the term of the agreement, BA shall notify CE within twenty-four (24) hours of any suspected or actual breach of security, intrusion, or unauthorized use or disclosure of PHI, PI, or PII of which BA becomes aware and/or any actual or suspected use or disclosure of data in violation of any applicable federal or state laws or regulations. BA shall take (i) prompt corrective action to cure any such deficiencies and (ii) any action pertaining to such unauthorized disclosure required by applicable federal and state laws and regulations (including conducting a “risk of compromise” assessment and/or appropriate patient notification under applicable state and/or federal law). For specific instruction on breach notification, see **Exhibit E, “Privacy and Information Security Provisions.”**

11. Breach Pattern or Practice by CE. Pursuant to 42 USC Section 17934(b), if BA knows of a pattern of activity or practice of CE that constitutes a material breach or violation of the CE’s obligations under the agreement or Addendum or other arrangement, BA must take reasonable steps to cure the breach or end the violation. If the steps are unsuccessful, BA must terminate the agreement if feasible, or if termination is not feasible, report the problem to the Secretary of DHHS. BA shall provide written notice to CE of any pattern of activity or practice of CE that BA believes constitutes a material breach or violation of CE’s obligations under the agreement or Addendum or other arrangement within five (5) days of discovery and shall meet with CE to discuss and attempt to resolve the problem as one of the reasonable steps to cure the breach or end the violation.

12. Audits, Inspection and Enforcement. Within ten (10) days of a written request by CE, BA and its agents or subcontractors shall allow CE to conduct a reasonable inspection of the facilities, systems, books, records, agreements, information systems, policies, and procedures relating to the use or disclosure of PHI, PI, or PII pursuant to this Addendum for the purpose of determining whether BA has complied with this Addendum; provided, however, that (i) BA and CE shall mutually agree in advance upon the scope, timing, and location of such an inspection; (ii) CE shall protect the confidentiality of all confidential and proprietary information of BA to which CE has access during the course of such inspection; and (iii) CE shall execute a nondisclosure agreement, upon terms mutually agreed upon by the parties, if requested by BA. A. The fact that CE inspects, or fails to inspect, or has the right to inspect, BA’s facilities, systems, books, records, agreements, policies, and procedures does not relieve BA of its responsibility to comply with this Addendum, nor does CE’s (i) failure to detect or (ii) detection, but failure to notify BA or require BA’s remediation of any unsatisfactory practices, constitute acceptance of such practice or a waiver of CE’s enforcement rights under the agreement or Addendum. BA shall notify CE within ten (10) days of learning that BA has become the subject of an audit, compliance review, or complaint investigation by the Office of Civil Rights.

13. PROVISIONS FOR CE TO INFORM BA OF PRIVACY PRACTICES AND RESTRICTIONS

A. CE shall notify BA of any limitation(s) in the Notice of Privacy Practices of CE under [45 CFR 164.520](#), to the extent that such limitation(s) may affect BA’s use or disclosure of PHI.

B. CE shall notify BA of any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI, to the extent that such changes may affect BA’s use or disclosure of PHI.

C. CE shall notify BA of any restriction on the use or disclosure of PHI that CE has agreed to or is required to abide by under [45 CFR 164.522](#), to the extent that such restriction may affect BA’s use or disclosure of PHI.

14. TERMINATION

A. Material Breach. A breach by BA of any provision of this Addendum, as determined by CE, shall constitute a material breach of the agreement and shall provide grounds for immediate termination of the agreement, any provision in the agreement to the contrary notwithstanding. [[45 CFR Section 164.504\(e\)\(2\)\(iii\)](#)].

B. Judicial or Administrative Proceedings. CE may terminate the agreement, effective immediately, if (i) BA is named as a defendant in a criminal proceeding for a violation of HIPAA, the HITECH Act, the HIPAA Regulations, or other security or privacy laws or (ii) a finding or stipulation that the BA has violated any standard or requirement of HIPAA, the HITECH Act, the HIPAA Regulations, or other security or privacy laws is made in any administrative or civil proceeding in which BA has been joined.

C. Obligations of BA Upon Termination. Upon termination of this agreement for any reason, BA, with respect to PHI, PI, or PII received from CE, or created, maintained, or received by BA on behalf of CE, shall:

1. Retain only that PHI, PI, or PII which is necessary for BA to continue its proper management and administration or to carry out its legal responsibilities;
2. Return to CE the remaining PHI, PI, or PII that the BA still maintains in any form;
3. Continue to use appropriate safeguards and comply with [Subpart C of 45 CFR Part 164](#) with respect to electronic PHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as BA retains the PHI;
4. Not use or disclose the PHI, PI, or PII retained by BA other than for the purposes for which such PHI, PI, or PII was retained and subject to the same conditions set out in this agreement above which applied prior to termination; and
5. Return to CE or, if agreed to by CE, destroy the PHI, PI, and PII retained by BA when it is no longer needed by BA for its proper management and administration or to carry out its legal responsibilities.

15. INDEMNIFICATION: BA agrees to indemnify, defend, and hold harmless CE and CE's agents, board members, elected and appointed officials and officers, employees, volunteers, and authorized representatives from any and all losses, liabilities, charges, damages, claims, liens, causes of action, awards, judgments, costs, and expenses (including, but not limited to, reasonable attorneys' fees of County Counsel and counsel retained by CE, expert fees, costs of staff time, and investigation costs) of whatever kind or nature, which arise out of or are in any way connected with any negligent act or omission of BA or BA's officers, agents, employees, independent BAs, subcontractor of any tier, or authorized representatives. Without limiting the generality of the foregoing, the same shall include injury or death to any person or persons; damage to any property, regardless of where located, including the property of CE; and any workers' compensation claim or suit arising from or connected with any services performed pursuant to this agreement on behalf of BA by any person or entity.

16. DISCLAIMER: CE makes no warranty or representation that compliance by BA with this Addendum, HIPAA, the HITECH Act, or the HIPAA Regulations will be adequate or satisfactory for BA's own purposes. BA is solely responsible for all decisions made by BA regarding the safeguarding of PHI.

17. CERTIFICATION: To the extent that CE determines that such examination is necessary to comply with CE's legal obligations pursuant to HIPAA relating to certification of its security practices, CE or its authorized agents or contractors, may, at CE's expense, examine BA's facilities, systems, procedures, and records as may be necessary for such agents or contractors to certify to CE the extent to which BA's security safeguards comply with HIPAA, the HITECH Act, the HIPAA Regulations, or this Addendum.

18. AMENDMENT: The parties acknowledge that state and federal laws relating to data security and privacy are rapidly evolving and that amendment of the agreement or Addendum may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule, and other applicable laws relating to the security or confidentiality of PHI. The parties understand and agree that CE must receive satisfactory written assurance from BA that BA will adequately safeguard all PHI. Upon the request of either party, the other party agrees to promptly enter into negotiations concerning the terms of an amendment to this Addendum embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule, or other applicable laws. CE may terminate the agreement upon thirty (30) days' written notice in the event (i) BA does not promptly enter into negotiations to amend the agreement or Addendum when requested by CE pursuant to this Section or (ii) BA does not enter into an amendment to the agreement or Addendum providing assurances regarding the safeguarding of PHI that CE, in its sole discretion, deems sufficient to satisfy the standards and requirements of applicable laws.

19. ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS: BA shall make itself, and any subcontractors, employees, or agents assisting BA in the performance of its obligations under the agreement or Addendum, available to CE, at no cost to CE, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CE, its directors, officers, or employees based upon a claimed violation of HIPAA, the HITECH Act, The Privacy Rule, the Security Rule, or other laws relating to security and privacy, except where BA or its subcontractor employee or agent is a named adverse party.

20. NO THIRD-PARTY BENEFICIARIES: Nothing expressed or implied in the agreement or Addendum is intended to confer, nor shall anything herein confer, upon any person other than CE, BA, and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

21. EFFECT ON AGREEMENT: Except as specifically required to implement the purposes of this Addendum, or to the extent inconsistent with this Addendum, all other terms of the agreement shall remain in force and effect.

22. INTERPRETATION: The provisions of this Addendum shall prevail over any provisions in the agreement that may conflict or appear inconsistent with any provision in this Addendum. This Addendum and the agreement shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, the Privacy Rule, and the Security Rule. The parties agree that any ambiguity in this Addendum shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act, the Privacy Rule, and the Security Rule.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

CASO DOCUMENT MANAGEMENT, INC

DOCUMENT MANAGEMENT COMPREHENSIVE SOFTWARE SOLUTIONS FOR DOCUMENT SCANNING, ELECTRONIC DOCUMENT MANAGEMENT, AND CONTRACT LIFE CYCLE MANAGEMENT

EXHIBIT E - PRIVACY AND INFORMATION SECURITY PROVISIONS

This Exhibit is intended to protect the privacy and security of specified Kern Behavioral Health and Recovery Services (County) information that Contractor may access, receive, or transmit under this agreement. County information covered under this Exhibit consists of: (1) Protected Health Information (PHI) as defined under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191; (2) Personal Information (PI) as defined under the California Information Practices Act (CIPA), at California Civil Code Section 1798.3; Personal Information may include data provided to the Department by the Social Security Administration; and (3) Personally Identifiable Information (PII); however, to the extent that data is PHI or ePHI and PI or PII, this Exhibit shall apply.

1. RECITALS.

A. In addition to the Privacy and Security Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which defines Protected Health Information (PHI), County is subject to various other legal and contractual requirements with respect to the personal information (PI) and personally identifiable information (PII) it maintains. These include:

1. The California Information Practices Act of 1977 (California Civil Code §§ 1798 et seq.).
2. The Agreement between the Social Security Administration (SSA) and the Department of Health Care Services (DHCS), known as the Information Exchange Agreement (IEA), which incorporates the Computer Matching and Privacy Protection Act Agreement (CMPPS) between the SSA and the California Health and Human Services Agency.
3. Title 42 Code of Federal Regulations, Chapter I, Subchapter A, Part 2.
4. California Welfare and Institutions Code § 5328 et seq.

B. The terms used in this Exhibit but not otherwise defined, shall have the same meanings as those terms have in the above referenced statute and agreement. Any reference to statutory, regulatory, or contractual language shall be to such language as in effect or as amended.

C. For the purpose of this Exhibit, PHI, PI, and PII all refer to confidential information that must be protected.

2. DEFINITIONS.

A. Breach shall have the meaning given to such term under the IEA, CMPPA and under HIPAA, the HITECH Act, and the HIPAA regulations at 45 C.F.R §164.402. It shall include a security incident, intrusion, or unauthorized access, use or disclosure of County PHI, ePHI, PI or PII.

B. Breach of the security of the system shall have the meaning given to such term under the California Information Practices Act, Civil Code section 1798.29(f).

C. CMPPA agreement means the Computer Matching and Privacy Protection Act agreement between the Social Security Administration and the California Health and Human Services Agency (CHHS).

D. Confidential Information: Information that is exempt from disclosure under the provisions of the California Public Records Act (Government Code sections 6250-6265) or other applicable state or federal laws.

E. Department PI shall mean Personal Information, accessed in a database maintained by County, received by Contractor from County or acquired or created by Contractor in connection with performing the functions, activities and services specified in this agreement on behalf of County.

F. Notice-triggering Personal Information shall mean the personal information identified in Civil Code section 1798.29 whose unauthorized access may trigger notification requirements under Civil Code section 1798.29. For purposes of this provision, identity shall include, but not be limited to, name, address, email address, identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print, a photograph, or a biometric identifier. Notice-triggering Personal Information includes PI in electronic, paper, or any other medium.

G. Personally Identifiable Information (PII): Any information about an individual which can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, and biometric records. This information can be in paper or electronic files and includes, but is not limited to, education records, financial transactions, employment history, criminal records, and medical files.

H. Personal Information (PI): Information that identifies or describes an individual, including, but not limited to, name, social security number, physical description, address, telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual.

I. Protected Health Information (PHI): Individually identifiable health information that is transmitted or maintained in any form or medium, created or received by a health care provider or health plan, that relates to past, present, and future physical or mental health condition of an individual; provisions of healthcare to an individual; or past, present and future payment for the provision of healthcare to an individual. Health information which is considered subject to the regulations contained in the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) including: name, date of birth, telephone number, names of relatives, names of employers, photographic images, facsimile number, medical record number, finger or voice prints, certificate/license number, social security number, internet (IP) address, web URL, e-mail address, and any device or serial number. "Protected Health Information" includes electronic protected health information.

J. Public Information: Information that is not exempt from disclosure under the provisions of the California Public Records Act (Government Code sections 6250-6265) or other applicable state or federal laws.

K. Required by law means a mandate contained in law that compels an entity to make a use or disclosure of PI or PII that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants, subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information, and a civil or an authorized investigative demand. It also includes Medicare conditions of participation with respect to health care providers participating in the program, and

statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

L. Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI, PI, PII or confidential data utilized in complying with this Agreement; or interference with system operations in an information system that processes, maintains or stores P H I , PI, or PII.

M. Sensitive Information: Information that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion. Sensitive information may be either public information or confidential information. It is information that requires a higher than normal assurance of accuracy and completeness. Thus, the key factor for sensitive information is that of integrity. Typically, sensitive information includes records of agency financial transactions and regulatory actions.

1. Contractor and its employees, agents, or subcontractors shall promptly transmit to the County Contract Manager all requests for disclosure of any PHI, PI, or PII not emanating from the person who is the subject of PHI, PI, or PII without a signed Consent for Release of Information.

2. Contractor shall not disclose, except as otherwise specifically permitted by this agreement or authorized by the person who is the subject of PHI, PI, or PII, any PHI, PI, or PII to anyone other than County without prior written authorization from the County Contract Manager, except if disclosure is required by state or federal law.

3. TERMS OF AGREEMENT

A. Permitted Uses and Disclosures of KernBHRS PHI, PI, and PII by Contractor:

1. Except as otherwise indicated in this Exhibit, Contractor may use or disclose Department PHI, PI, and/or PII only to perform functions, activities, or services for or on behalf of KernBHRS pursuant to the terms of this agreement provided that such use or disclosure would not violate the California Information Practices Act (CIPA) if done by KernBHRS.

2. Contractor shall not directly or indirectly receive remuneration in exchange for County PHI.

B. Responsibilities of Contractor

Contractor agrees:

1. Nondisclosure. To protect from unauthorized disclosure any Sensitive or Confidentiality information. Not to use or disclose KernBHRS PHI, PI, or PII other than in carrying out the Contractor's obligations under this agreement or as permitted or required by applicable state and federal law.

2. Safeguards. To implement appropriate and reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of KernBHRS PHI, PI, and PII, to protect against anticipated threats or hazards to the security or integrity of KernBHRS PHI, PI, and PII, and to prevent use or disclosure of KernBHRS PHI, PI, or PII other than as provided for by this agreement. Contractor shall develop and maintain a written privacy and information security program that include administrative, technical, and physical safeguards appropriate to the size and complexity of Contractor's operations and the nature and scope of its activities. Contractor will provide KernBHRS with its current policies upon request.

3. Security. Contractor shall take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI, PI, and/or PII, and to protect paper documents containing PHI, PI, and/or PII. These steps shall include, at a minimum:

A. Complying with all of the data system security precautions listed in Business Associate Agreement Data Security Requirements.

B. Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A- 130, Appendix III- Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in federal agencies.

4. Mitigation of Harmful Effects. To mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of KernBHRS PHI, PI, or PII by Contractor or its subcontractors in violation of this Exhibit.

5. Contractor's Agents and Subcontractors. To impose the same restrictions and conditions set forth in this Exhibit on any subcontractors or other agents with whom Contractor subcontracts any activities under this agreement that involve the disclosure of Department PHI, PI, or PII to the subcontractor.

6. Availability of Information to County. To make County PHI, PI, and PII available to County for purposes of oversight, inspection, amendment, and response to requests for records, injunctions, judgments, and orders for production of County PHI, PI, and PII. If Contractor receives County PHI, PI, and/or PII, upon request by County, Contractor shall provide County with a list of all employees, contractors, and agents who have access to County PHI, PI and/or PII, including employees, contractors, and agents of its subcontractors and agents.

7. Cooperation with County. With respect to County PHI, PI, and/or PII, to cooperate with and assist County to the extent necessary to ensure County's compliance with the applicable terms of the California Information Practice Act including, but not limited to, accounting of disclosures of County PHI, PI, and/or PII, correction of errors in County PHI, PI, and/or PII, production of County PHI, PI, and/or PII, disclosure of a security breach involving County PHI, PI, and/or PII, and notice of such breach to the affected individual(s).

8. Confidentiality of Substance Use Disorder and Treatment Records. Contractor agrees to comply with all confidentiality requirements set forth in Title 42 Code of Federal Regulations, Chapter I, Subchapter A, Part 2. Contractor is aware that criminal penalties may be imposed for a violation of these confidentiality requirements.

4. SAFEGUARDS.

Contractor shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI, PI, and/or PII, including electronic PHI, PI, and/or PII that it creates, receives, maintains, uses, or transmits on behalf of County. Contractor shall develop and maintain a written information privacy and security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the Contractor's operations and the nature and scope of its activities, including at a minimum the following safeguards:

4.1. Personnel Controls

a. **Employee Training.** All workforce members must complete privacy and information security training through the Relias training system, upon hire and annually thereafter. If Contractor does not have access to Relias, Contractor will need to document their staff's training attendance, including maintaining a sign-in sheet, e-sign or certificate, indicating the staff member's name and the date on which the training was completed. These certifications must be retained for a period of ten (10) years following contract termination. Contractor will need to develop an internal tracking mechanism to monitor their staff's attendance. This tracking system shall be available for the County to review at any time, to ensure that this required training is completed. Contractor's Privacy and Information Security training must consist of the following:

1. HIPAA Privacy and Security regulations (45 CFR Part 160 and 164)
2. California Welfare and Institutions Code § 5328 et seq (required if Contractor provides mental health services)
3. Title 42 Code of Federal Regulations, Chapter I, Subchapter A, Part 2 (required if Contractors provides any substance use services, even if Contractor is a primary mental health provider).
4. Contractor's internal policies and procedures related to sections 1-3 above.

a. **Employee Discipline.** Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.

b. **Confidentiality Statement.** All persons that will be working with County PHI, PI, and/or PII must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to being provided access to Department PHI, PI, or PII. The statement must be renewed annually. Contractor shall retain each person's written confidentiality statement for County inspection for a period of six (6) years following contract termination.

c. **Background Check.** Before a member of the workforce may access County PHI, PI, and/or PII, a thorough background check of that worker must be conducted, with evaluation of the results to assure that there is no indication that the worker may present a risk to the security or integrity of confidential data or a risk for theft or misuse of confidential data. Contractor shall retain each workforce member's background check documentation for a period of three (3) years following contract termination.

4.2. Technical Security Controls

a. **Workstation/Laptop encryption.** All workstations and laptops that process and/or store County PHI, PI, and/or PII must be encrypted using a FIPS 140-2 certified algorithm which is 128-bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the County Information Security Officer.

b. **Server Security.** Servers containing unencrypted County PHI, PI, and/or PII must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

c. **Minimum Necessary.** Only the minimum necessary amount of County PHI, PI, and/or PII required to

perform necessary business functions may be copied, downloaded, or exported.

d. Removable media devices. All electronic files that contain County PHI, PI, and/or PII data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, Smart Phone, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128-bit or higher, such as AES.

e. Antivirus software. All workstations, laptops and other systems that process and/or store County PHI, PI, and/or PII must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

f. Patch Management. All workstations, laptops and other systems that process and/or store County PHI, PI, and/or PII must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within thirty (30) days of vendor release.

g. User IDs and Password Controls. All users must be issued a unique username for accessing County PHI, PI, and/or PII. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within twenty four (24) hours. Passwords are not to be shared. Passwords must be at least ten (10) characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every ninety (90) days, preferably every sixty (60) days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three (3) of the following four groups from the standard keyboard:

- Upper case letters (A-Z)
- Lower case letters (a-z)
- Arabic numerals (0-9)
- Non-alphanumeric characters (punctuation symbols)

h. Data Destruction. When no longer needed, all County PHI, PI, and/or PII must be wiped using the Gutmann or U.S. Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission of the County Information Security Officer.

i. System Timeout. The system providing access to County PHI, PI, and/or PII must provide an automatic timeout, requiring re-authentication of the user session after no more than fifteen (15) minutes of inactivity.

j. Warning Banners. All systems providing access to County PHI, PI, and/or PII must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.

k. System Logging. The system must maintain an automated audit trail which can identify the user or system process which initiates a request for County PHI, PI, and/or PII, or which alters County PHI, PI, and/or PII. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If County PHI, PI, and/or PII is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least three (3) years after occurrence. Audit Trail logs must be reviewed for potential violations and/or

breaches on a regular basis.

l. Access Controls. The system providing access to County PHI, PI, and/or PII must use role-based access controls for all user authentications, enforcing the principle of least privilege.

m. Transmission Encryption. All data transmissions of County PHI, PI, and/or PII outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128-bit or higher, such as AES. Encryption can be end-to-end at the network level, or the data files containing PHI, PI, or PII can be encrypted. This requirement pertains to any type of PHI, PI, or PII in motion such as website access, file transfer, and E-Mail. Any transmission of unencrypted PHI, PI and/or PII outside of Contractor's secure network, must be reported to the KernBHRS Privacy and Corporate Compliance office. (Contacts are listed at the end of this Exhibit).

n. Intrusion Detection. All systems involved in accessing, holding, transporting, and protecting County PHI, PI, and/or PII that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

4.3. Business Continuity / Disaster Recovery Controls

a. Emergency Mode Operation Plan. Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic County PHI, PI, and/or PII 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.

b. Data Backup Plan. Contractor must have established documented procedures to back up County PHI, PI, and/or PII to maintain retrievable exact copies of County PHI, PI, and/or PII. The plan must include a regular schedule for making backups, storing back-ups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore County PHI, PI, and/or PII should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of County data.

4.4. Paper Document Controls

a. Supervision of Data. County PHI, PI, and/or PII in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk, or office. Unattended means that information is not being observed by an employee authorized to access the information. County PHI, PI, and/or PII in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

b. Escorting Visitors. Visitors to areas where County PHI, PI, and/or PII is contained shall be escorted and County PHI, PI, and/or PII shall be kept out of sight while visitors are in the area.

c. Confidential Destruction. County PHI, PI, and/or PII must be disposed of through confidential means, such as cross-cut shredding and pulverizing.

d. Removal of Data. County PHI, PI, and/or PII must not be removed from the premises of Contractor except with express written permission of County.

e. Faxing. Faxes containing County PHI, PI, and/or PII shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving

faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.

f. Mailing. Mailings of County PHI, PI, and/or PII shall be sealed and secured from damage or inappropriate viewing of PHI, PI, or PII to the extent possible. Mailings which include five hundred (500) or more individually identifiable records of County PHI, PI, and/or PII in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of County to use another method is obtained.

4.5. Audit Controls

A. System Security Review. All systems processing and/or storing County PHI, PI and/or PII must have at least an annual system risk assessment/security review that provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.

1. Log Reviews. All systems processing and/or storing County PHI, PI, and/or PII must have a routine procedure in place to review system logs for unauthorized access.

2. Change Control. All systems processing and/or storing County PHI, PI, and/or PII must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity, and availability of data.

3. Receiving and Investigating Privacy Issues. Contractor shall have a process for staff or individuals to make complaints or report privacy issues. Contractors must document all complaints received and privacy issues investigated, including their disposition. Contractor shall provide to County, documentation of privacy issues investigated, upon request. Additionally, Contractor must submit a quarterly report, utilizing **Exhibit F, "Privacy and Compliance Investigation Summary,"** to the KernBHRS Privacy and Corporate Compliance office within thirty (30) calendar days of the end of each fiscal quarter.

B. Security Officer. Contractor shall designate an Information Security Officer to oversee its data security program who will be responsible for carrying out its privacy and security programs and for communicating on security matters with County, under 45 CFR 164.308.

C. Privacy Officer. Contractor shall designate a Privacy official who is responsible for the development and implementation of HIPAA policies and procedures per 45 CFR § 164.530(a)(1)(i). Contractor must designate a contact person or office who is responsible for receiving complaints under 45 CFR § 164.530(a)(1)(ii).

D. Discovery and Notification of Breach. Contractor shall notify County **immediately by telephone call and email** upon the discovery of a breach (or suspected breach) of privacy or security of PHI, PI, and/or PII in electronic, paper, spoken or in any other media, if the PHI, PI, and/or PII was not securely transmitted, or is reasonably believed to have been, accessed, acquired by an unauthorized person, or upon the discovery of a suspected privacy or security incident that involves data provided to County by the Social Security Administration or involving County PHI, PI, and/or PII; **or by email within twenty-four (24) hours** of the discovery of any suspected security incident, intrusion, or unauthorized use or disclosure of PHI, PI, and/or PII in violation of this agreement or the Business Associate Agreement, or potential loss of confidential data affecting this agreement. A breach shall be treated as discovered by Contractor as of the first day on which the breach is known, or by exercising reasonable diligence, would have been known, to any person (other than the

person committing the breach) who is an employee, officer, or other agent of Contractor.

Notification shall be provided to the KernBHRS Contract Manager, the KernBHRS Privacy & Corporate Office, and the KernBHRS Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves electronic PHI, PI, and/or PII, notification shall be provided by calling the KernBHRS Information Security Officer at (661) 203-5397. Alternately, contact the KernBHRS Information Technology Services Division (ITSD) Help Desk at 661-868-6740. Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use, or disclosure of PHI, PI, and/or PII, Contractor shall take:

1. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the Contractor's operating environment and information confidentiality and security requirements.
2. Any action pertaining to such unauthorized disclosure required by applicable federal and state laws and regulations.

E. Investigation of Breach. In the event Contractor's actions or inactions cause a security incident, breach or unauthorized use or disclosure of PHI, PI, and/or PII, Contractor shall immediately investigate such security incident, breach, or unauthorized use or disclosure of PHI, PI, and/or PII and within **forty eight (48)** hours of the discovery, Contractor shall submit an initial Department of Health Care Services (DHCS) "Privacy Incident Report," containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time. Contractor shall use the most current version of this form, which is posted on the DHCS Information website <https://www.dhcs.ca.gov/formsandpubs/laws/priv/Documents/Privacy-Incident-Report-PIR.pdf>. Submit this report to the KernBHRS Privacy and Corporate Compliance Office via email at BHRSPrivacy@KernBHRS.org.

F. Written Report. Contractor shall provide a final written report of the investigation to the KernBHRS Privacy Office within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on the DHCS "Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "Privacy Incident Report" form. KernBHRS Privacy Office will submit this information to DHCS, who will review and approve the determination of whether a breach occurred and whether individual notification is required. Contractor shall also submit, to the KernBHRS Privacy Office, an internal incident or investigation report, completed by Contractor.

G. Notification of Individuals. In the event Contractor's actions or inactions cause a breach or unauthorized use or disclosure of PHI, PI, and/or PII, Contractor shall notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal law, and shall pay any costs of such notifications, as well as any costs associated with the breach.

1. Once DHCS has made a breach determination, Contractor shall draft a (de-identified) proposed breach notification letter, using guidelines provided in the [SIMM 5340-C](#) (State of California, California Information Security Office: Requirements to Respond to Incidents Involving a Breach of Personal Information), as instructed, and submit to the KernBHRS Privacy Office, who will submit the letter to DHCS for approval.

2. When the proposed breach notification letter is approved by DHCS, KernBHRS Privacy Office or designee will notify Contractor, who shall then proceed with mailing the notification letter(s) to the affected beneficiary/beneficiaries without reasonable delay, and in no event later than sixty (60) calendar days following the date of discovery.

3. Contractor shall notify the Department of Health and Human Services (HHS), Office for Civil Rights (OCR) no later than sixty (60) days after the end of the calendar year in which the breach is discovered, for a breach affecting less than five hundred (500) individuals, by visiting the HHS website (https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true) and filling out and electronically submitting a breach report form. If the breach affects five hundred (500) or more individuals, the KernBHRS Privacy Office will coordinate next steps with Contractor, including HHS notification.

H. Effect on lower tier transactions. The terms of this Exhibit shall apply to all contracts, subcontracts, and subawards, regardless of whether they are for the acquisition of services, goods, or commodities. Contractor shall incorporate the contents of this Exhibit into each subcontract or subaward to its agents, subcontractors, or independent consultants.

I. Contact Information. To direct communications to the below referenced KernBHRS staff, Contractor shall initiate contact as indicated herein. KernBHRS reserves the right to make changes to the contact information below by giving written notice to Contractor. Said changes shall not require an amendment to this Exhibit or the agreement into which it is incorporated.

Kern Behavioral Health and Recovery Services Contract Manager	Kern Behavioral Health and Recovery Services Privacy Officer	Kern Behavioral Health and Recovery Services Information Security Officer
Name: Rachelle Hunt E-Mail: RHunt@kernbhers.org Phone: (661) 868-7752 Kern Behavioral Health and Recovery Services P.O. Box 1000 Bakersfield, CA 93302	Privacy & Corporate Compliance Officer Elizabeth Brown Email: EBrown@KernBHRS.org Direct Line: 661-868-6821 Kern Behavioral Health and Recovery Services P.O. Box 1000 Bakersfield, CA 93302 Privacy and Corporate Compliance Office Telephone: (661) 868-6868 Email: BHRSPrivacy@KernBHRS.org	Information Security Officer Rachelle Hunt Email: RHunt@KernBHRS.org Kern Behavioral Health and Recovery Services P.O. Box 1000 Bakersfield, CA 93302 Help Desk Telephone: (661) 868-6740 Email: BHRSHelpDesk@KernBHRS.org

J. Audits and Inspections. From time to time, KernBHRS may inspect the facilities, systems, books and records of Contractor to monitor compliance with the safeguards required in this Exhibit. Contractor shall promptly remedy any violation of any provision of this Privacy and Information Security Exhibit. The fact that KernBHRS inspects, or fails to inspect, or has the right to inspect Contractor's facilities, systems, and procedures does not relieve Contractor of its responsibility to comply with this Exhibit.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

CASO DOCUMENT MANAGEMENT, INC**DOCUMENT MANAGEMENT COMPREHENSIVE SOFTWARE SOLUTIONS FOR DOCUMENT
SCANNING, ELECTRONIC DOCUMENT MANAGEMENT, AND CONTRACT LIFE CYCLE
MANAGEMENT****EXHIBIT F - PRIVACY AND COMPLIANCE INVESTIGATION SUMMARY****NOTE: COMPLETED COPY ON FILE WITH PRIVACY AND CORPORATE COMPLIANCE**

Contractor must provide this summary to the KernBHRS Privacy and Corporate Compliance office by email @ BHRSPrivacy@KernBHRS.org, within thirty (30) calendar days of the end of each fiscal quarter. Please keep in mind that privacy and compliance investigations do not have a negative impact. Investigating privacy and compliance issues and following up on issues/risks identified are a way to show that a Privacy or Compliance Program is effective.

Report for: FY _____ ☐☐☐☐☐ Qtr. 1 (July-Sept) ☐☐☐☐☐ Qtr. 2 (Oct-Dec) ☐☐☐☐☐ Qtr. 3 (Jan-Mar) ☐☐
☐☐ Qtr. 4 (Apr-Jun)

Contractor Name: _____

Contractor Address: _____

Name of Privacy Officer: _____

Phone: _____ Email: _____

Name of Compliance Officer: _____

Phone: _____ Email: _____

Name of Information Security Officer: _____

Phone: _____ Email: _____

PRIVACY INVESTIGATIONS:

Total Privacy investigations this quarter: _____

Total investigations this quarter resulting in a breach: _____

Breach(es) reported to KernBHRS ☐☐☐ Yes ☐☐☐ No

Please list the types of Privacy investigations conducted below (e.g. inappropriate access, inappropriate disclosure, PHI lost/stolen, misdirected mail/fax, unencrypted PHI in email, etc.). Enter total number of each type of investigation.

Type of Investigation	Total	Type of Investigation	Total
-----------------------	-------	-----------------------	-------

COMPLIANCE INVESTIGATIONS:

Total Compliance investigations this quarter: _____

Total investigations this quarter resulting in fraud, waste or abuse: _____

Fraud, waste or abuse reported to KernBHRS ☐☐☐ Yes ☐☐☐ No

Please list the types of Compliance investigations conducted (e.g. policy violation, code of ethics violation, questionable billing practice, allegation of fraud, waste or abuse, etc.). Enter total number of each type of investigation.

Type of Investigation	Total	Type of Investigation	Total
-----------------------	-------	-----------------------	-------

Signature _____ Title _____

Name (please print) _____ Date _____

CASO DOCUMENT MANAGEMENT, INC**COMPREHENSIVE SOFTWARE SOLUTIONS FOR DOCUMENT SCANNING, ELECTRONIC
DOCUMENT MANAGEMENT, AND CONTRACT LIFE CYCLE MANAGEMENT****EXHIBIT G - DISCLOSURE OF OWNERSHIP AND CONTROL INTEREST STATEMENT****NOTE: COMPLETED COPY ON FILE WITH CONTRACT MONITORING TEAM**

The federal regulations set forth in [42 CFR 455.101](#), [455.104](#), [455.105](#), [455.106](#), and [455.434](#) require providers who are entering into or renewing a provider agreement to disclose to the U.S. Department of Health and Human Services, the state Medicaid agency, and to Managed Care Organizations that contract with the state Medicaid Agency: 1) the identity of all owners with a control interest of five percent **(5%) or greater**, 2) certain business transactions as described in 42 CFR 455.105 and 3) the identity of any excluded individual or entity with an ownership or control interest in the provider, the provider group, or disclosing entity or who is an agent or managing employee of the provider group or entity or who is an agent or managing employee of the provider entity and 4) arrange for fingerprint clearance for criminal background checks and submit proof of clearance along with Disclosure of Ownership and Control Interest Statement documentation. Any changes in ownership during the contract year will require all documentation to be updated.

Please attach a separate sheet if necessary.

Provider Entity Information
Circle the Type of disclosing entity:
☐ Individual Member of a Group or Sole Proprietor ☐ Partnership ☐ Corporation ☐ Limited Liability
☐ Other (Specify) _____
Legal Name of individual or entity ("Provider Entity"):
DBA Name:
Group Name:
Primary/Main Office Address:
Mailing Address (if different from above)
Practice Address 1:
Practice Address 2:
Federal Tax Identification #:
Medicaid ID#:
National Provider ID (NPI) #:
Provider CAQH #:

***If applicable, add the group, provider or health care professional name and EIN when the Provider Entity is part of a group practice, attach a separate sheet if necessary.**

Section I						
Are there any individuals or organizations with an Ownership or Control Interest of 5% or more in the Provider Entity? ☐ Yes ☐ No						
List the name, title, address, date of birth (DOB) and Social Security Number (SSN) for all individuals having an <u>ownership or control interest in the Provider Entity of 5% or greater</u> . This Should match those listed in the organizational chart. For Owners list the percentage of ownership. Attach additional pages if needed to identify all parties with ownership or control interest.						
List the name, Tax Identification Number (TIN), business address of each organization, corporation, or entity having an ownership of corporation, or entity having an Ownership or Control Interest of 5% or greater . (42 CFR 455.104 (b) (1) (ii))						
Name/Title	DOB	Address (Address Line)	Address (City, State & Zip Code)	SSN (if listing an individual)	TIN (if listing an entity)	% Interest

Section II

Are any of the individuals listed in Section I above related to each other? ___ **Yes** ___ **No**

If yes, list the individuals identified and the relationship to each other (spouse, sibling, parent, child).

Are any individuals listed in Section I above related to any individuals with an ownership or control interest in any of the subcontractors listed in Section III below? ___ **Yes** ___ **No**

If yes, list their name and relationship. ([42 CFR.455.104 \(b\) \(2\)](#))

Name Of Individuals	Relationships

Section III

Does the Provider Entity have a Direct or Indirect Ownership Interest in any Subcontractor 5% or more that another individual or organization also has an Ownership or Controlling Interest? ___ **Yes** ___ **No**

If yes, list the following information for each person with an Ownership or controlling Interest in any Subcontractor in which the Provider Entity has Direct or Indirect Ownership of 5% or more. ([42 CFR 455.104](#))

Name/Title	Address	DOB	SSN (if listing an individual) TIN (if listing an entity)	% Interest

Section IV

Has any person who has an ownership or control interest in the provider entity, or is an agent or managing employee of the Provider Entity ever been convicted of a crime related to that person's involvement in any program under Medicaid, Medicare or Title XX program? ___ **Yes** ___ **No** (verify through HHS-OIG List of Excluded individuals/Entities (LEIE), General Services Administration (GSA) Excluded Parties List (EPLS), the Medicare Exclusion Database (the MED) databases and any State specific database.)

Any person who has a 5% or more direct or indirect interest must also submit fingerprints and a background check.

If yes, please list those persons below. ([42 CFR 455.106](#))

Name/Title	DOB	Address	SSN (if listing an individual) TIN (if listing an entity)

Section V

Business Transactions: Has the provider Entity had any business transactions with Subcontractors or Wholly Owned Supplier totaling more than \$25,000 or 5% or operating expenses in the previous twelve (12) month period ___ **Yes** ___ **No**

If yes, list the ownership of Subcontractor with whom the Provider Entity has had a business transaction totaling more than \$25,000 during the previous twelve 12-month period; and any Significant Business Transaction between this provider and any wholly owned supplier exceeding the lesser of \$25,000 or 5% operating expense, during the past 5-year period. This information must be provided within 35 days of the request.

Attach a separate sheet if necessary.

([42 CFR 455.104](#) and [42 CFR 455.105](#))

Name of Supplier/ Subcontractor	Address	Owner	SSN (if listing an individual) TIN (if listing an entity)	Transaction Amount
--	----------------	--------------	--	-------------------------------

Section VI				
Managing Employees: Does the Provider Entity have any Managing Employees? __Yes __No				
If yes, for Disclosing Entities, list each member of the Board of Directors, Governing Board, and Managing Employees (general manager, business manager, administrator or director), including the name, date of birth (DOB), Address, Social Security Number (SSN), and percent of interest.				
Name of Supplier/ Subcontractor	Address	Owner	SSN (if listing an individual) TIN (if listing an entity)	Transaction Amount

I certify that the information provided herein, is true, accurate and complete.

Any person who has a 5% or more direct or indirect interest must also submit fingerprints and the background check results with the Disclosure of Ownership form.

Additions or revisions to the information above will be submitted immediately upon revision. Additionally, I understand that misleading, inaccurate, or incomplete data may result in a denial of participation. Individuals and Sole Proprietors must sign their own form. An authorized representative may sign for Partnership, Corporation, LLC or Other disclosing entities.

Contractor: Click or tap here to enter text.

Signature: Click or tap here to enter text.

Print: Click or tap here to enter text.

Title: Click or tap here to enter text.

Date: Click or tap here to enter text.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

CASO DOCUMENT MANAGEMENT, INC

COMPREHENSIVE SOFTWARE SOLUTIONS FOR DOCUMENT SCANNING, ELECTRONIC DOCUMENT MANAGEMENT, AND CONTRACT LIFE CYCLE MANAGEMENT

EXHIBIT H - QUALIFIED SERVICES ORGANIZATION AGREEMENT

CASO Document Management, Inc. ("Contractor") and County Of Kern ("County") hereby enter into an agreement, whereby the Contractor agrees to provide document scanning, data migration, EasyFile configuration and implementation, workflow and contract lifecycle management functionality, system integrations, training, technical support, and ongoing platform maintenance.

Furthermore, CASO:

1. Acknowledges that in receiving, transmitting, transporting, storing, processing, or otherwise dealing with any information received from the County identifying or otherwise relating to the patients in the County ("protected information"), it is fully bound by the provisions of the federal regulations governing the [Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2](#); and the Health Insurance Portability and Accountability Act (HIPAA), [45 C.F.R. Parts 160, 162 and 164](#);
2. Agrees to resist any efforts in judicial proceedings to obtain access to the protected information except as expressly provided for in the regulations governing the Confidentiality of Alcohol and Drug Abuse Patient Records, [42 C.F.R. Part 2](#);
3. Agrees that it will not use or disclose protected health information except as permitted or required by this Agreement or by law;
4. Agrees that, when the Contractor uses, discloses, or requests protected health information, it will limit the use, disclosure, or request to the minimum necessary;
5. Agrees that if the Contractor enters into a contract with any agent, including a subcontractor, the agent will agree to comply with [42 C.F.R. Part 2 and HIPAA](#), and, if the Contractor learns of a pattern or practice by the agent that is a material breach of the contract with the Contractor, to take reasonable steps to cure the breach or terminate the contract, if feasible;
6. Agrees to comply with HIPAA's security provisions with regard to electronic protected health information, and to use appropriate safeguards, including the safeguards described in Exhibits D and E of this agreement, to prevent the unauthorized use or disclosure of the protected information;
7. Agrees to report breaches of protected information to the County;
8. Agrees to report to the County any use or disclosure of the protected information not provided for in this Agreement of which it becomes aware;
9. Agrees to ensure that any agent, including a subcontractor, to whom the Contractor provides protected information received from the County, or creates or receives on behalf of the County, agrees to the same restrictions and conditions that apply through this Agreement to the Contractor with respect to such information;
10. Agrees to provide access to the protected information at the request of the County, or to an individual as directed by the County, in order to meet the requirements of [45 C.F.R. §164.524](#)

which provides patients with the right to access and copy their own protected information;

11. Agrees to make any amendments to the protected information as directed or agreed to by the County pursuant to [45 C.F.R. §164.526](#);

12. Agrees to make available its internal practices, books, and records, including policies and procedures, relating to the use and disclosure of protected information received from the County, or created or received by the Contractor on behalf of the County, to the County or to the Secretary of the Department of Health and Human Services for purposes of the Secretary determining the County's compliance with HIPAA;

13. Agrees to document disclosures of protected information, and information related to such disclosures, as would be required for the County to respond to a request by an individual for an accounting of disclosures in accordance with [45 C.F.R. §164.528](#);

14. Agrees to provide the County or an individual information in accordance with paragraph (13) of this agreement to permit the County to respond to a request by an individual for an accounting of disclosures in accordance with [45 C.F.R. §164.528](#);

Termination

1. The County may terminate this Agreement if it determines that the Contractor has violated any material term.

2. Upon termination of this Agreement for any reason, the Contractor shall return or destroy all protected information received from the County or created or received by the Contractor on behalf of the County. This provision shall apply to protected information that is in the possession of subcontractors or agents of the Contractor. The Contractor shall retain no copies of the protected information.

3. In the event that the Contractor determines that returning or destroying the protected information is infeasible, the Contractor shall notify the County of the conditions that make return or destruction infeasible.

4. Upon notification that the return or destruction of the protected information is infeasible, the Contractor shall extend the protections of this Agreement to such protected information and limit further uses and disclosures of the information to those purposes that make the return or destruction infeasible, as long as the Contractor maintains the information.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

CASO DOCUMENT MANAGEMENT, INC

COMPREHENSIVE SOFTWARE SOLUTIONS FOR DOCUMENT SCANNING, ELECTRONIC DOCUMENT MANAGEMENT, AND CONTRACT LIFE CYCLE MANAGEMENT

EXHIBIT J – EASYFILE® MASTER SUBSCRIPTION AGREEMENT

Cloud Document Management Platform — Subscription Services Agreement

CASO Document Management, Inc. • 134 West 29th Street, 11th Floor, New York, NY 10001

These Master Subscription Terms (the "Agreement") govern Customer's subscription to and use of the EasyFile cloud document management platform and related services provided by CASO Document Management, Inc. ("CASO"). This Agreement is effective as of the effective date of the first Order Form referencing it (the "Effective Date") and is entered into between CASO and the customer entity identified on such Order Form ("Customer"). Each Order Form, together with this Agreement and its Schedules, forms a single integrated agreement.

1. DEFINITIONS

"AI Services" means optional artificial-intelligence features of the Subscription Service, including the EasyFile AI Connector, made available under the AI Services Addendum (Schedule B) when purchased or enabled on an Order Form.

"Authorized User" means an individual employee, contractor, volunteer, or agent of Customer who is authorized by Customer to access the Subscription Service under Customer's subscription, up to the number of users specified in the applicable Order Form.

"Available" has the meaning given in Schedule A.

"Customer Data" means all documents, images, files, metadata, form submissions, workflow data, audit logs, and other electronic data uploaded to or generated within the Subscription Service by or on behalf of Customer or its Authorized Users.

"Documentation" means CASO's then-current user guides, administrator guides, API documentation, and technical documentation for the Subscription Service.

"Order Form" means an ordering document executed by both parties that specifies the Subscription Service tier, number of Authorized Users, optional modules, fees, Subscription Term, and Customer elections, and that references this Agreement.

"Professional Services" means implementation, configuration, migration, integration, training, or other consulting services described in an Order Form or statement of work.

"Schedules" means Schedule A (Service Levels, Support, and Recovery), Schedule B (AI Services Addendum), and Schedule C (Security and Compliance Summary), each of which is incorporated into this Agreement by reference.

"Security Incident" means a confirmed unauthorized acquisition, access, use, or disclosure of Customer Data. Unsuccessful attempts that do not result in unauthorized access — including routine scans, pings, and blocked login attempts — are not Security Incidents.

"Subscription Service" means the EasyFile cloud-hosted document management platform, including EasyFile Workflow, EasyFile Capture, Smart Forms, and other modules identified on an Order Form, together with the Documentation.

"Subscription Term" means the initial subscription period stated in the Order Form and each renewal period.

2. THE SUBSCRIPTION SERVICE

2.1 Access Grant. Subject to Customer's payment of applicable fees and compliance with this Agreement, CASO grants Customer a non-exclusive, non-transferable right during the Subscription Term for its Authorized Users to access and use the Subscription Service for Customer's internal business purposes, in accordance with the Documentation and the applicable Order Form.

2.2 Modules Included. The Order Form states the modules included in Customer's subscription. No per-module, per-feature, or per-transaction fee applies to any module listed in the Order Form during the Subscription Term.

2.3 Authorized Users. Access credentials are for named Authorized Users and may not be shared. Customer may reassign a credential from one individual to another. Customer is responsible for all activity occurring under its Authorized Users' accounts and for the accuracy of user counts. If actual usage exceeds the subscribed user tier, the parties will execute an amended Order Form at the then-applicable tier.

2.4 Environments. CASO will provision and maintain two environments for Customer throughout the Subscription Term: a Production environment and a User Acceptance Testing ("UAT") environment. Material updates and new features are deployed to UAT for Customer validation before promotion to Production, except emergency security patches under Section 2.6.

2.5 Updates. CASO may enhance, update, and modify the Subscription Service from time to time, provided no such change materially degrades the core functionality of the Subscription Service during a paid Subscription Term. Customer's administrators may enable or hold back individual features on a per-cabinet or per-feature basis where the Subscription Service provides that control.

2.6 Maintenance. CASO will provide Customer's designated administrators at least seventy-two (72) hours' advance notice by email of scheduled maintenance. Scheduled maintenance is performed during the maintenance window stated in Schedule A. Emergency security patches may be applied with as much advance notice as is reasonably practicable.

2.7 API Stability. CASO will maintain backward compatibility for Customer's existing API integrations. CASO will provide Customer at least ninety (90) days' advance written notice before any breaking change to, or deprecation of, any REST API endpoint or version in use by Customer, and will provide a migration guide. CASO will support concurrent API versions during any transition period. API documentation, code samples, SDKs, and a Postman collection are provided at no additional charge and kept current.

2.8 Professional Services. Professional Services, where purchased, are described in the applicable Order Form or statement of work and are performed in a professional and workmanlike manner. Changes to agreed scope require a written change order signed by both parties.

2.9 Restrictions. Customer will not, and will not permit any third party to: (a) sublicense, resell, rent, or otherwise make the Subscription Service available to any third party except as expressly permitted;

(b) reverse engineer, decompile, or attempt to derive source code from the Subscription Service; (c) use the Subscription Service to build a competing product; (d) circumvent usage limits or security controls; (e) upload malicious code; or (f) use the Subscription Service in violation of applicable law. Access by Customer's contractors and agents acting on Customer's behalf, and by other Customer departments as stated in the Order Form, is not a violation of this Section.

3. TERM AND RENEWAL

3.1 Agreement Term. This Agreement commences on the Effective Date and continues while any Order Form remains in effect.

3.2 Subscription Term; Renewal. The Subscription Term is stated in the Order Form. **This Agreement does not automatically renew.** Renewal requires a renewal Order Form or written amendment signed by both parties before expiration. CASO will provide renewal pricing at least ninety (90) days before the end of the then-current Subscription Term.

3.3 Effect of Non-Renewal. Upon expiration of the Subscription Term without renewal, all rights to access and use the Subscription Service terminate in full, subject only to the data export period in Section 5.3. Customer retains no license, hosted environment, or right of access after expiration.

4. FEES AND PAYMENT

4.1 Fees. Customer will pay the fees stated in each Order Form. Except as expressly provided in this Agreement, **fees are non-cancelable and payment obligations are non-refundable.**

4.2 Invoicing and Payment Terms. Unless the Order Form states otherwise, subscription fees are invoiced annually in advance and Professional Services are invoiced as described in the Order Form. Invoices are due net thirty (30) days from the invoice date. Late amounts may accrue interest at the lesser of 1.5% per month or the maximum rate permitted by law.

4.3 Taxes. Fees are exclusive of taxes. Customer is responsible for all applicable sales, use, and similar taxes, excluding taxes based on CASO's income. Tax-exempt Customers will provide a valid exemption certificate.

4.4 Suspension for Non-Payment. CASO may suspend access to the Subscription Service if undisputed fees remain unpaid thirty (30) days after written notice of delinquency. Suspension does not relieve Customer of its payment obligations, and CASO will promptly restore access upon payment.

5. CUSTOMER DATA

5.1 Ownership. As between the parties, Customer owns all right, title, and interest in and to Customer Data. CASO acquires no rights in Customer Data other than the limited right to host, process, transmit, display, secure, back up, and support Customer Data as necessary to provide the Subscription Service and as otherwise instructed by Customer.

5.2 Data Export During the Term. The Subscription Service provides self-service export of documents, associated metadata, and audit logs at any time during the Subscription Term at no additional charge.

5.3 Data Export at Termination. For sixty (60) days following expiration or termination of the final Order Form, CASO will, upon Customer's written request, make Customer Data available for export in industry-standard formats (documents as PDF/A or in their stored native format; metadata and audit logs as CSV or JSON). After such sixty (60) day period, CASO will have no obligation to retain Customer Data and will delete or de-identify Customer Data in accordance with its data retention practices, except as required by law, legal hold, or a written agreement with Customer. Assisted export services beyond self-service tooling, if requested, are available as Professional Services.

5.4 Role of the Parties. Customer determines the purposes and means of processing Customer Data. CASO processes Customer Data only to provide the Subscription Service, Professional Services, support, security, backup, disaster recovery, and other services documented in this Agreement or Customer's written instructions.

5.5 Prohibited Uses. CASO will not:

- (a) sell or share Customer Data;
- (b) use Customer Data for cross-context behavioral advertising;
- (c) retain, use, or disclose Customer Data outside the direct business relationship with Customer or for any purpose other than performing the services;
- (d) use Customer Data, or any output derived from Customer Data, to train, fine-tune, or improve any artificial-intelligence or machine-learning model, whether CASO's own or a third party's; or
- (e) combine Customer Data with data from any other source, except as necessary to provide the services to Customer.

5.6 Regulated Data. Where Customer Data includes data subject to sector-specific regulation, the parties' obligations with respect to that data are governed by separately executed agreements between the parties, including any Business Associate Agreement or Qualified Service Organization Agreement. In the event of a conflict, those agreements control with respect to the data each covers.

5.7 Data Location. The Subscription Service is hosted in United States data center regions. CASO will not store, host, or process Customer Data outside the United States without Customer's prior written consent.

5.8 Subprocessors.

- (a) CASO's current subprocessors are listed in Schedule C.
- (b) CASO will impose written data protection obligations on each subprocessor that are no less protective in material respects than those in this Agreement, taking into account the nature of the services provided by the subprocessor.
- (c) CASO will provide Customer at least thirty (30) days' prior notice before adding or replacing a subprocessor with access to Customer Data. Customer may object on reasonable data protection grounds during the notice period, in which case the parties will work in good faith to identify a commercially reasonable alternative.
- (d) Emergency substitutions necessary to preserve service security, availability, or legal compliance may occur without prior notice, provided CASO notifies Customer as soon as reasonably practicable.

5.9 Audit Logs. The Subscription Service maintains an audit log of user and administrative activity. Customer may export the audit log using available self-service export tools during the Subscription Term at no additional charge.

5.10 Usage Data. CASO may collect and use technical and operational data regarding use of the Subscription Service (excluding Customer Data content) to operate, secure, support, and improve the Subscription Service.

6. SECURITY AND COMPLIANCE

6.1 Security Program. CASO maintains a written information security program with administrative, physical, and technical safeguards designed to protect the security, confidentiality, and integrity of Customer Data, including encryption of Customer Data at rest (AES-256) and in transit (TLS 1.2 or higher), logical per-tenant data isolation, role-based access controls, and audit logging. Controls are summarized in Schedule C.

6.2 Independent Attestation. CASO maintains a SOC 2 Type II attestation covering the Security and Availability trust services criteria for its document imaging and enterprise content management systems and will, upon written request and subject to confidentiality obligations, make its then-current report available to Customer no more than once annually.

6.3 Hosting Infrastructure. The Subscription Service is hosted on Microsoft Azure. Azure serves as a subservice organization and maintains its own independent certifications and attestations covering the infrastructure layer.

6.4 Incident Notification. CASO will notify Customer without undue delay, and in no event later than twenty-four (24) hours, after confirming a Security Incident. CASO's notice will include information reasonably available at the time regarding the nature and scope of the incident, the affected systems and data, containment actions taken, and planned remediation, and CASO will supplement the notice as further information becomes available. CASO will reasonably cooperate with Customer's investigation of and response to a Security Incident.

6.5 Security Documentation. Upon written request and subject to confidentiality obligations, CASO will provide a security review package including SOC 2 report access, an infrastructure summary, a data flow overview, the subprocessor list, an incident response summary, and standard security questionnaire responses.

6.6 Service Levels. Availability, support, performance standards, backup, and recovery objectives are governed by Schedule A.

7. AI SERVICES

7.1 Optional Services. AI Services are optional and are provided only if purchased or enabled on an Order Form, subject to the AI Services Addendum (Schedule B). Customer administrators control which cabinets, document types, and workflows are eligible for AI processing, and may disable AI features on a per-feature or per-cabinet basis or globally at any time.

7.2 AI Providers. AI Services are delivered under either the CASO-Managed Model or the BYOK Model, as described in Schedule B. Customer elects the deployment model on the Order Form. Where Customer elects the bring-your-own-key (BYOK) model, Customer's own agreement with its chosen AI provider governs that provider's processing, and Customer is responsible for maintaining that relationship and associated keys.

7.3 AI Output. AI-generated output is probabilistic and may contain errors. The Subscription Service routes low-confidence results for human review in accordance with Customer's configuration, as described in Schedule B.

7.4 No Training. CASO does not use Customer Data or AI output to train, fine-tune, or improve any model, as stated in Section 5.5(d).

8. CONFIDENTIALITY

8.1 Definition. "Confidential Information" means non-public information disclosed by one party to the other that is designated confidential or that reasonably should be understood to be confidential given its nature and the circumstances of disclosure. Customer's Confidential Information includes Customer Data; CASO's Confidential Information includes the Subscription Service, Documentation, pricing, security reports, and non-public operating procedures.

8.2 Obligations. The receiving party will use the disclosing party's Confidential Information only to perform under this Agreement, will protect it using at least the same degree of care it uses for its own similar information (and no less than reasonable care), and will not disclose it except to employees, contractors, and advisors with a need to know who are bound by obligations at least as protective. These obligations survive for five (5) years after disclosure; obligations with respect to Customer Data and trade secrets survive indefinitely.

8.3 Exclusions; Compelled Disclosure. Confidential Information does not include information that is or becomes public through no fault of the receiving party, was known without restriction before disclosure, is independently developed, or is rightfully received from a third party. A party may disclose Confidential Information as required by law or legal process, provided it gives prompt notice (where legally permitted) and reasonable cooperation to seek protective treatment. For public sector Customers, the parties acknowledge that this Agreement and related records may be subject to applicable freedom-of-information or public records laws.

9. INTELLECTUAL PROPERTY

9.1 CASO Ownership. CASO and its licensors own all right, title, and interest in and to the Subscription Service, the Documentation, and all related software, technology, templates, configurations, code, and know-how, including all improvements and derivatives. No rights are granted to Customer except as expressly stated in this Agreement.

9.2 Customer Ownership. Customer owns Customer Data and Customer-specific work product expressly identified as Customer-owned in an Order Form or statement of work.

9.3 Feedback. Customer may provide suggestions or feedback regarding the Subscription Service. CASO may use feedback without restriction or obligation, provided it does not identify Customer without consent.

10. WARRANTIES AND DISCLAIMERS

10.1 Mutual Warranties. Each party represents and warrants that it has the legal power to enter into this Agreement and that the person executing each Order Form is authorized to do so.

10.2 Service Warranty. CASO warrants that during the Subscription Term the Subscription Service will perform materially in accordance with the Documentation, and that Professional Services will be performed in a professional and workmanlike manner. Customer's exclusive remedy for breach of this warranty is re-performance or repair by CASO and, if CASO cannot remedy the non-conformity within a reasonable period, termination of the affected Order Form and a pro-rata refund of prepaid, unused fees for the affected service.

10.3 Disclaimer. EXCEPT AS EXPRESSLY STATED IN THIS AGREEMENT, THE SUBSCRIPTION SERVICE IS PROVIDED "AS IS" AND CASO DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, AND ANY WARRANTY THAT THE SUBSCRIPTION SERVICE WILL BE UNINTERRUPTED OR ERROR-FREE. OCR, DATA EXTRACTION, AND AI ACCURACY DEPEND ON SOURCE DOCUMENT QUALITY AND REQUIRE CUSTOMER VALIDATION WORKFLOWS. THIRD-PARTY INTEGRATIONS DEPEND ON THE CONTINUED AVAILABILITY OF THIRD-PARTY APIS AND EXPORT ACCESS.

11. INDEMNIFICATION

11.1 By CASO. CASO will defend Customer against any third-party claim alleging that the Subscription Service, as provided by CASO and used in accordance with this Agreement, infringes a United States patent, copyright, or trademark, or misappropriates a trade secret, and will indemnify Customer for damages, costs, and reasonable attorneys' fees finally awarded or agreed in settlement. If the Subscription Service becomes, or in CASO's opinion is likely to become, the subject of such a claim, CASO may procure the right for Customer to continue using it, modify or replace it with functionally equivalent service, or, if neither is commercially reasonable, terminate the affected Order Form and refund prepaid, unused fees. This Section states CASO's entire liability, and Customer's exclusive remedy, for infringement claims. CASO has no obligation for claims arising from Customer Data, combination with items not provided by CASO, modifications not made by CASO, or use in violation of this Agreement.

11.2 By Customer. To the extent permitted by applicable law (and, for governmental entities, subject to the limits of applicable state or local law regarding indemnification by public bodies), Customer will defend CASO against third-party claims arising from Customer Data or Customer's use of the Subscription Service in violation of this Agreement or applicable law, and will indemnify CASO for damages, costs, and reasonable attorneys' fees finally awarded or agreed in settlement.

11.3 Procedure. The indemnified party must promptly notify the indemnifying party of the claim, grant sole control of the defense and settlement (provided any settlement fully releases the indemnified party without admission of fault), and provide reasonable cooperation at the indemnifying party's expense.

12. LIMITATION OF LIABILITY

12.1 Exclusion of Consequential Damages. TO THE MAXIMUM EXTENT PERMITTED BY LAW, NEITHER PARTY WILL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES, OR FOR LOST PROFITS, LOST REVENUE, OR LOSS OF BUSINESS, HOWEVER CAUSED AND UNDER ANY THEORY OF LIABILITY, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

12.2 General Liability Cap. TO THE MAXIMUM EXTENT PERMITTED BY LAW, AND EXCEPT AS STATED IN SECTION 12.3, EACH PARTY'S TOTAL AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT WILL NOT EXCEED THE TOTAL FEES PAID OR PAYABLE BY CUSTOMER UNDER THE APPLICABLE ORDER FORM IN THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE FIRST EVENT GIVING RISE TO LIABILITY.

12.3 Data Breach Super-Cap. FOR A SECURITY INCIDENT CAUSED BY CASO OR ITS SUBPROCESSORS, CASO'S TOTAL AGGREGATE LIABILITY WILL NOT EXCEED **TWO TIMES (2x)** THE TOTAL FEES PAID OR PAYABLE BY CUSTOMER UNDER THE APPLICABLE ORDER FORM IN THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE INCIDENT.

12.4 Exceptions. The limitations in this Section 12 do not apply to: (a) Customer's payment obligations; (b) a party's indemnification obligations under Section 11; or (c) a party's gross negligence, willful misconduct, or fraud.

13. TERMINATION

13.1 Termination for Cause. Either party may terminate this Agreement or any Order Form upon written notice if the other party materially breaches this Agreement and fails to cure the breach within thirty (30) days after written notice describing the breach.

13.2 Termination for Insolvency. Either party may terminate upon written notice if the other party becomes the subject of a petition in bankruptcy or any proceeding relating to insolvency, receivership, or assignment for the benefit of creditors that is not dismissed within sixty (60) days.

13.3 Termination for Service Failure. Customer may terminate as provided in Schedule A for sustained failure to meet the Uptime Commitment.

13.4 Effect of Termination. Upon expiration or termination: (a) Customer's access rights end, subject to the data export period in Section 5.3; (b) Customer will pay all fees accrued through the effective date of termination; and (c) if Customer terminates for CASO's uncured material breach or under Section 13.3, CASO will refund prepaid fees covering the remainder of the terminated Subscription Term.

13.5 Survival. Sections 1, 3.3, 5.1, 5.3, 5.5, 5.10, 8, 9, 10.3, 11, 12, 13.4, 13.5, and 15 survive termination.

14. PUBLIC SECTOR CUSTOMERS; CHANNEL PARTNERS

14.1 Order of Precedence. In the event of a conflict, the following order of precedence applies: (a) any government-mandated terms expressly incorporated into a signed Order Form or mutually executed contract amendment; (b) the Order Form; (c) any executed Business Associate Agreement or Qualified Service Organization Agreement, with respect to the regulated data each covers; (d) Schedule B (AI Services Addendum), with respect to AI Services; (e) the remaining Schedules; and (f) these Master Subscription Terms. Government or procurement terms bind CASO only if expressly incorporated by reference in a document signed by both parties; terms contained in purchase orders, vendor portals, or click-through registrations are of no effect.

14.2 Public Sector Accommodations. For Customers that are governmental entities, the parties acknowledge that certain provisions of this Agreement may be superseded by non-waivable

requirements of applicable law (including public records laws, non-appropriation of funds, and indemnification limits). Where Customer's enabling law prohibits a provision of this Agreement, that provision is deemed modified to the minimum extent necessary to comply, and the remainder of this Agreement remains in effect. Multi-year Subscription Terms for governmental Customers are subject to annual appropriation of funds where required by law; Customer will provide prompt written notice of non-appropriation, and termination for non-appropriation will be treated as expiration, without penalty, effective at the end of the last funded period.

14.3 Channel Partners. Customer may procure its subscription through a CASO-authorized reseller or channel partner identified on the Order Form. In such case, the reseller handles ordering and billing, but this Agreement governs Customer's access to and use of the Subscription Service directly between CASO and Customer, including the service levels, data protection, and security commitments herein. No reseller is authorized to modify this Agreement or make representations or warranties on CASO's behalf, and any such statements are void.

15. GENERAL

15.1 Governing Law; Venue. This Agreement is governed by the laws of the State of New York, without regard to conflicts of law principles, and the parties consent to the exclusive jurisdiction of the state and federal courts located in New York County, New York.

15.2 Assignment. Neither party may assign this Agreement without the other party's prior written consent, except that either party may assign it in connection with a merger, acquisition, or sale of substantially all assets, with written notice to the other party.

15.3 Force Majeure. Neither party is liable for delay or failure to perform (other than payment obligations) caused by events beyond its reasonable control, including natural disasters, acts of government, labor disputes, utility or internet failures, and denial-of-service or similar attacks, provided the affected party uses reasonable efforts to mitigate.

15.4 Notices. Legal notices must be in writing and delivered by certified mail, nationally recognized courier, or email with confirmation of receipt, to the addresses stated on the Order Form. Operational notices (including maintenance and incident notices) may be provided through the Subscription Service or by email to the Customer administrator.

15.5 Insurance. During the Subscription Term, CASO will maintain commercially reasonable insurance coverage, including commercial general liability, professional liability (errors and omissions), and cyber liability coverage, and will provide certificates of insurance upon written request.

15.6 Publicity. Neither party will use the other party's name or logo publicly without prior written consent, except that CASO may identify Customer as a customer in factual lists of customers unless Customer opts out in writing.

15.7 Independent Contractors; No Third-Party Beneficiaries. The parties are independent contractors. This Agreement does not create any third-party beneficiary rights.

15.8 Waiver; Severability. A waiver is effective only if in writing. If any provision is held unenforceable, it will be modified to the minimum extent necessary, and the remainder of this Agreement remains in effect.

15.9 Entire Agreement; Amendments; Counterparts. This Agreement (including all Order Forms and Schedules) is the entire agreement between the parties regarding its subject matter and

supersedes all prior and contemporaneous agreements and communications. Amendments must be in a writing signed by both parties. Order Forms may be executed in counterparts, including by electronic signature.

SCHEDULES

Schedule	Title
Schedule A	Service Levels, Support, and Recovery
Schedule B	AI Services Addendum
Schedule C	Security and Compliance Summary

Signature block appears on the Order Form.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

CASO DOCUMENT MANAGEMENT, INC

COMPREHENSIVE SOFTWARE SOLUTIONS FOR DOCUMENT SCANNING, ELECTRONIC DOCUMENT MANAGEMENT, AND CONTRACT LIFE CYCLE MANAGEMENT

EXHIBIT K – SCHEDULE A — SERVICE LEVELS, SUPPORT, AND RECOVERY

EasyFile® Master Subscription Agreement

CASO Document Management, Inc.

This Schedule A is incorporated into the EasyFile Master Subscription Agreement (the "Agreement") between CASO Document Management, Inc. ("CASO") and Customer. Capitalized terms not defined here have the meanings given in the Agreement.

1. DEFINITIONS

1.1 "Available" means the Subscription Service is accessible and materially operable for its core functions, being: user authentication and login; document search; document retrieval and viewing; document upload and capture; and workflow task processing. The Subscription Service is not Available if any core function is inoperable or materially degraded for substantially all Authorized Users, notwithstanding that the login endpoint responds.

1.2 "Business Hours" means Monday through Friday, 8:00 AM to 6:00 PM Eastern Time, excluding holidays observed by CASO, unless different hours are stated in the Order Form.

1.3 "Business Day" means any day on which Customer's offices are open for business.

1.4 "Downtime" means the total minutes in a calendar month during which the Subscription Service is not Available, excluding Excluded Downtime.

1.5 "Excluded Downtime" means unavailability caused by:

- (a) Scheduled Maintenance conducted in accordance with Section 4;
- (b) emergency maintenance reasonably required to protect the security or integrity of the Subscription Service;
- (c) factors outside CASO's reasonable control, including force majeure events, general internet outages, and failures of Customer's equipment, software, or network connectivity;
- (d) Customer's acts or omissions, or those of a third party acting on Customer's behalf, including misuse of the Subscription Service;
- (e) failure or degradation of a third-party integration, API, or AI provider **that Customer supplies, designates, or controls**, including the status of any Customer-supplied AI credential or endpoint; or
- (f) suspension of the Subscription Service as permitted by the Agreement.

1.6 "Monthly Uptime Percentage" means, for a calendar month:

(total minutes in the month – Excluded Downtime – Downtime) ÷ (total minutes in the month – Excluded Downtime), expressed as a percentage.

1.7 "Scheduled Maintenance" means maintenance announced in accordance with Section 4.

2. AVAILABILITY

2.1 Uptime Commitment. CASO will make the Subscription Service Available with a Monthly Uptime Percentage of at least 99.9% in each calendar month (the "Uptime Commitment").

2.2 Measurement. Availability is measured by CASO's monitoring systems. CASO will make monitoring data supporting any month's calculation available to Customer on request. If Customer's own monitoring materially conflicts with CASO's, the parties will review the underlying data in good faith.

2.3 Availability Information. On Customer's written request, CASO will provide availability information for the preceding calendar quarter, including Monthly Uptime Percentage and a summary of any Downtime.

3. SERVICE CREDITS

3.1 Credit Schedule. If the Monthly Uptime Percentage falls below the Uptime Commitment, Customer is eligible for a Service Credit calculated as a percentage of the monthly subscription fee for that month, being the annual subscription fee divided by twelve:

Monthly Uptime Percentage	Service Credit
Below 99.9% but at or above 99.0%	5% of monthly fee
Below 99.0% but at or above 95.0%	10% of monthly fee
Below 95.0%	15% of monthly fee

3.2 Claim Procedure. To receive a Service Credit, Customer must submit a written request to CASO support within thirty (30) days after the end of the calendar month in which the Uptime Commitment was not met, including the dates and times of the claimed unavailability. CASO will validate claims against its monitoring data.

3.3 Application and Cap. Service Credits are applied against the next invoice or, if no further invoice will be issued, refunded within sixty (60) days. **Service Credits for any single calendar month will not exceed fifteen percent (15%) of that month's subscription fee, and Service Credits in any twelve (12) month period will not exceed, in the aggregate, one hundred percent (100%) of one month's subscription fee.**

3.4 Relationship to Other Remedies. Service Credits are Customer's exclusive monetary remedy for failure to meet the Uptime Commitment alone. **Service Credits do not limit, waive, or substitute for Customer's rights and remedies** for breach of any other provision of the Agreement or applicable law, including remedies for data loss or security incidents.

3.5 Termination for Sustained Failure. If the Monthly Uptime Percentage falls below 95.0% in each of three (3) consecutive calendar months, **Customer may terminate the Order Form on thirty (30) days' written notice** and receive a pro-rata refund of prepaid, unused fees. This right is in addition to Service Credits.

4. MAINTENANCE

4.1 Advance Notice. CASO will give Customer's designated administrators and project sponsor **at least seventy-two (72) hours' advance notice by email** of scheduled maintenance, stating the window, expected impact, and affected functions.

4.2 Maintenance Window. Scheduled maintenance is performed during CASO's standard maintenance window: **Saturday 11:00 PM to Sunday 3:00 AM Eastern Time**. Where maintenance is reasonably necessary outside that window, CASO will provide notice under Section 4.1.

4.3 Emergency Maintenance. Emergency security patches may be applied with as much notice as is reasonably practicable. CASO will notify Customer of the reason and impact as soon as possible and in all events within twenty-four (24) hours.

4.4 UAT First. Material updates and new features are deployed to Customer's UAT environment for validation before promotion to Production, except emergency security patches under Section 4.3. Customer's administrators receive advance UAT access to new features.

5. SUPPORT

5.1 Channels. CASO provides support by telephone, email, and online ticketing portal during Business Hours. The online ticketing portal is available 24x7 for submission, status tracking, and access to the knowledge base. Severity 1 incidents may be reported 24x7 through the designated emergency contact process. Email support is acknowledged within twenty-four (24) hours.

5.2 Severity Levels and Response Targets.

Severity	Definition	Target Response Initial	Resolution Target
1 — Critical	Subscription Service unavailable or unusable for substantially all	2 Business Hours (24x7 reporting)	Same Business Day, or a written escalation plan by end of that Business Day

	Authorized Users; no workaround		
2 — Major	Core feature materially impaired; workaround difficult or unavailable	4 Business Hours	Next Business Day
3 — Standard	Non-critical issue or question; reasonable workaround exists	Next Business Day	Within 5 Business Days
4 — Enhancement	Feature request or enhancement	5 Business Days	Scheduled in a future release or addressed by change order

5.3 Proactive Incident Notification. CASO monitors the Subscription Service and Azure infrastructure continuously. Where CASO detects a Severity 1 or Severity 2 incident affecting Customer, CASO will notify Customer's designated administrators promptly, whether or not Customer has reported it.

5.4 Escalation Path. Unresolved issues escalate as follows: support ticket → CASO support management → engineering lead → Technical Lead → President and CEO. Contact details are stated in the Order Form. Customer may invoke escalation at any time.

5.5 Status Updates. CASO will provide status updates on open Severity 1 and Severity 2 incidents at intervals appropriate to the severity.

5.6 Support Hours. Support is provided during Business Hours as defined in Section 1.2. Extended support hours and after-hours coverage are available as options and, where purchased, are stated in the Order Form.

6. DOCUMENTATION AND KNOWLEDGE RESOURCES

6.1 Materials. The Subscription Service includes role-specific user guides, an administrator reference guide, release notes, and a searchable online knowledge base accessible to all Authorized Users. CASO keeps these materials current with the Subscription Service.

6.2 Training. Training services, including implementation training, administrator training, and any recurring or refresher training, are provided as described in the Order Form or an applicable statement of work.

7. BACKUP AND RECOVERY

7.1 Backups. CASO performs automated backups of Customer Data and the configuration data required to restore the Subscription Service, stored using geographically redundant Azure storage within the United States.

7.2 Retention.

Backup Type	Frequency	Retention
Daily	At least once per calendar day	30 days
Weekly	At least once per calendar week	12 weeks
Monthly	At least once per calendar month	12 months
Annual archive	Optional, only if stated in the Order Form	Up to 7 years

7.3 Integrity. Backup integrity is verified through periodic restoration testing. Point-in-time recovery is available within the retention period.

7.4 Recovery Objectives.

Objective	Commitment
Recovery Point Objective (RPO)	24 hours
Recovery Time Objective (RTO)	4 Business Hours for critical restoration

7.5 Disaster Recovery Testing. CASO tests its disaster recovery procedures **at least annually**, covering complete environment failure with alternate-region restoration, database corruption with point-in-time recovery, and application-tier failover.

7.6 DR Test Documentation. CASO documents the results of each disaster recovery test, including scope, scenarios exercised, results measured against the objectives in Section 7.4, and findings. CASO makes this documentation available to Customer on request and remediates material findings.

8. MONITORING

8.1 Continuous Monitoring. CASO monitors the Subscription Service and Azure infrastructure 24×7 using Azure Monitor, Application Insights, and CASO's internal monitoring stack, with automated alerting on failures, performance degradation, capacity thresholds, and security events.

8.2 Scope of Monitoring. Monitoring covers: indexing throughput, queue depth, error rate, and extraction confidence; OCR success rate, accuracy, and throughput, with failed documents flagged for

manual review; search response times with slow-query detection; and workflow stage transition times, task queue depth, escalation events, and bottlenecks. Results are surfaced in Customer's dashboards.

9. DATA EXPORT

Customer's data export rights during and after the Subscription Term are governed by Sections 5.2 and 5.3 of the Agreement.

10. CHANGES TO THIS SCHEDULE

CASO may update this Schedule from time to time, provided no update materially reduces the Uptime Commitment, Service Credit entitlements, standard support response targets, or stated recovery objectives applicable to Customer during a paid Subscription Term unless Customer agrees in writing.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

CASO DOCUMENT MANAGEMENT, INC

COMPREHENSIVE SOFTWARE SOLUTIONS FOR DOCUMENT SCANNING, ELECTRONIC
DOCUMENT MANAGEMENT, AND CONTRACT LIFE CYCLE MANAGEMENT

EXHIBIT L - SCHEDULE B — AI SERVICES ADDENDUM

EasyFile® Master Subscription Agreement

CASO Document Management, Inc.

This Schedule B is incorporated into the EasyFile Master Subscription Agreement (the "Agreement") and applies only if AI Services are enabled in the Order Form. Capitalized terms not defined here have the meanings given in the Agreement.

Precedence. Where this Schedule conflicts with the body of the Agreement with respect to AI Services, this Schedule controls, except that Sections 5.5, 5.6, and 5.7 of the Agreement control in all events.

1. DEFINITIONS

"AI Output" means content, classifications, extractions, summaries, answers, or other results generated by AI Services in response to Customer inputs.

"AI Provider" means the provider used to deliver AI Services under the CASO-Managed Model, or the Customer-designated provider under the BYOK Model.

"AI Services" means the optional artificial-intelligence features of the Subscription Service, including the EasyFile AI Connector, and functions such as classification, extraction, summarization, and question-answering.

"BYOK Model" means the deployment model in which Customer provides and controls the AI Provider account, endpoint, subscription, or API credential.

"CASO-Managed Model" means the deployment model in which CASO provides AI Provider access under CASO's own account.

"Foundation Model" means the underlying model used to generate AI Output.

2. AI FEATURES

The Subscription Service includes the following AI-enabled features:

Feature	Function
AI Connector	Connects the Subscription Service to a large language model provider by API, and

	governs how content is submitted and results returned
Capture AI	Field extraction and document classification for indexing
OCR	Optical character recognition and text extraction, performed by the document analysis service identified in Schedule C

Each feature may be enabled or disabled by Customer as provided in Section 3.3.

3. SCOPE, ACTIVATION, AND CUSTOMER CONTROL

3.1 Activation. AI Services are activated only for the features and deployment model stated in the Order Form.

3.2 Customer Control. Customer's administrators control which cabinets, document types, and workflows are eligible for AI processing. Content is submitted for AI processing only when Customer or an Authorized User invokes, schedules, or configures an AI-enabled function.

3.3 Disablement. Customer administrators may disable any AI feature, or all AI Services, on a per-feature, per-cabinet, or global basis at any time through configuration settings, without affecting the remainder of the Subscription Service and without charge. Deactivation does not relieve Customer of charges for usage already incurred.

3.4 Activation Authorization. AI Services are not activated in Production until Customer gives written authorization. Where Customer requires a security or AI governance review before activation, CASO will provide AI feature disclosure documentation covering feature inventory, data handling, model governance, security controls, third-party dependencies, and administrative opt-out settings.

3.5 Regulated Data. Customer determines whether particular categories of Customer Data are eligible for AI processing and configures eligibility accordingly. Where Customer Data is subject to sector-specific regulation, Customer is responsible for determining whether AI processing of that data is permitted under the agreements governing it.

4. DEPLOYMENT MODELS

4.1 CASO-Managed Model. Under the CASO-Managed Model:

- (a) CASO uses its own AI Provider account, and that provider is a CASO subprocessor identified in Schedule C;
- (b) CASO configures the AI Provider relationship to prohibit use of Customer Data and AI Output for model training, and will provide evidence of that configuration on request;

(c) CASO configures the AI Provider to minimize content retention to what is necessary to return AI Output, and will describe the applicable abuse-monitoring and content-retention configuration on Customer request; and

(d) **CASO will notify Customer in advance before materially changing the abuse monitoring or content retention configuration**, or before moving delivery of AI Services to a different account or subscription.

4.2 BYOK Model. Under the BYOK Model:

(a) Customer procures and maintains its own AI Provider account, endpoint, subscription, and credentials, and is responsible for provisioning, fees, usage limits, key security, and key rotation;

(b) Customer's own agreement with that provider governs the provider's processing of content, and that provider is **not** a CASO subprocessor;

(c) CASO transmits content to the Customer-designated endpoint solely at Customer's instruction and as configured by Customer, and CASO's processing in transit is limited to what is necessary to deliver the AI Services;

(d) CASO makes no representation or warranty regarding the Customer-designated provider's terms, data handling, security, availability, performance, or output; and

(e) unavailability or degradation of AI Services caused by that provider, or by the status of Customer's credential including suspension, quota exhaustion, or revocation, is not a failure of CASO's obligations and is Excluded Downtime under Schedule A.

4.3 Key Handling. CASO stores Customer-supplied API keys and endpoint credentials in encrypted form, uses them solely to deliver AI Services on Customer's behalf, does not disclose them to any third party, and deletes them on Customer's request or on termination of AI Services.

4.4 Model Substitution. CASO may substitute a Foundation Model or model version of materially equivalent or superior capability on notice to Customer, provided the substitution does not materially degrade the AI Services or reduce any data protection commitment.

5. DATA PROTECTION IN AI PROCESSING

5.1 No Training. CASO does not use Customer Data or AI Output to train, fine-tune, or improve any artificial-intelligence or machine-learning model, and contractually prohibits its AI Providers from doing so under the CASO-Managed Model. This restates and does not limit Section 5.5(d) of the Agreement.

5.2 Purpose Limitation. Content submitted to AI Services is transmitted to the configured AI Provider solely to generate and return AI Output.

5.3 Retention. CASO does not instruct, configure, or require the AI Provider to retain content beyond the processing necessary to return AI Output. Under the BYOK Model, Customer's own account configuration governs retention, abuse monitoring, and content filtering.

5.4 Document Analysis Services. OCR, text extraction, and layout analysis performed by document analysis services are governed by the applicable provider's data handling terms for those services, which are separate from Foundation Model terms. The provider used is identified in Schedule C.

5.5 Data Protection Terms Apply. AI processing of Customer Data is subject to Article 5 of the Agreement in full. **Nothing in this Schedule permits AI processing contrary to Customer’s instructions or to the agreements governing regulated Customer Data.**

5.6 Data Location. Section 5.7 of the Agreement applies to AI processing. **AI processing of Customer Data will occur within the United States.**

6. AI OUTPUT

6.1 Nature of AI Output. AI Output is generated by probabilistic models and may be inaccurate, incomplete, or unsuitable for Customer's purposes regardless of input quality. Accuracy depends on source document quality, legibility, and configuration.

6.2 Output Rights. As between the parties, Customer owns AI Output derived from Customer Data, subject to the applicable AI Provider's terms. Customer acknowledges AI-generated content may be similar to output generated for others and may not be subject to exclusive rights.

6.3 Confidence and Exception Handling. Where the Subscription Service assigns confidence scores to extraction or classification, low-confidence results are routed for human review in accordance with Customer's configuration.

7. ACCEPTABLE USE

Customer will use AI Services in compliance with applicable law, the Agreement, and the applicable AI Provider's acceptable use policies. Customer will not use AI Services to generate unlawful content or in any manner violating third-party rights.

8. USAGE AND FEES

8.1 BYOK Model. AI usage fees are billed directly to Customer by its own provider and are not included in CASO's subscription fees. **CASO applies no surcharge under the BYOK Model.**

8.2 CASO-Managed Model. AI usage is invoiced at **CASO's actual AI consumption cost plus a fifteen percent (15%) administrative fee**, unless the Order Form states another rate. CASO will provide supporting consumption detail with each invoice.

Deployment Model	Usage Charges
BYOK	Customer pays its provider directly. No CASO surcharge.

CASO-Managed	Actual consumption cost plus 15% administrative fee, unless the Order Form states another rate.
---------------------	--

8.3 Usage Reporting. CASO provides AI usage reporting based on available metering data on Customer's request.

8.4 Protective Throttling. CASO may temporarily throttle, suspend, or request confirmation for unusual or excessive AI usage to protect Customer from unexpected charges or to protect service integrity. **CASO will notify Customer promptly** and will not throttle in a manner that impairs non-AI functions of the Subscription Service.

9. DISCLAIMERS

IN ADDITION TO THE DISCLAIMERS IN THE AGREEMENT, CASO DOES NOT WARRANT THE ACCURACY, COMPLETENESS, FITNESS, OR AVAILABILITY OF ANY AI OUTPUT, AND UNDER THE BYOK MODEL MAKES NO WARRANTY REGARDING THE CUSTOMER-DESIGNATED AI PROVIDER OR ITS SERVICES.

This disclaimer does not limit CASO’s obligations under Sections 5.5, 5.6, and 5.7 of the Agreement or under Section 5 of this Schedule. CASO’s aggregate liability with respect to AI Services is subject to Section 12 of the Agreement.

10. TERM

This Schedule is coterminous with the Order Form under which AI Services are enabled. Customer may deactivate AI Services at any time under Section 3.3 without affecting the remainder of the Subscription Service.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

CASO DOCUMENT MANAGEMENT, INC

COMPREHENSIVE SOFTWARE SOLUTIONS FOR DOCUMENT SCANNING, ELECTRONIC DOCUMENT MANAGEMENT, AND CONTRACT LIFE CYCLE MANAGEMENT

EXHIBIT M - SCHEDULE C — SECURITY AND COMPLIANCE SUMMARY

EasyFile® Master Subscription Agreement

CASO Document Management, Inc.

This Schedule C is incorporated into the EasyFile Master Subscription Agreement (the "Agreement"). It summarizes CASO's security, compliance, and subprocessor practices for the EasyFile Subscription Service and may be shared with Customer's procurement, security, and compliance reviewers.

This Schedule is a summary. Where it differs from the operative commitments in the Agreement or Schedule A, those documents govern. Backup retention and recovery objectives are stated in Schedule A, Section 8, and are not restated here.

1. SERVICE OVERVIEW

EasyFile is CASO's cloud-hosted document management platform providing electronic document management, workflow automation, capture, Smart Forms, document viewing, redaction, integrations, reporting, and optional AI-enabled features. The modules included for Customer are stated in the Order Form.

2. HOSTING AND DATA RESIDENCY

2.1 Infrastructure. The Subscription Service is hosted on Microsoft Azure. Azure holds FedRAMP High Authorization, SOC 1/2/3, ISO 27001, and ISO 27017/27018 covering the infrastructure layer, and serves as a subservice organization with its own independent certifications.

2.2 Division of Responsibility. Azure provides the infrastructure layer. **CASO is responsible for the EasyFile application layer, configuration, support, and all customer-facing commitments in the Agreement.** CASO's SOC 2 Type II attestation covers the application layer using the carve-out method for Azure.

2.3 Data Residency. Production hosting is in **United States Azure regions**. Customer Data is not stored, hosted, or processed outside the United States. See Agreement, Section 5.7.

3. CONTROL SUMMARY

Control Area	EasyFile Practice
--------------	-------------------

Encryption at rest	Customer Data encrypted using AES-256 or equivalent Azure-managed encryption
Encryption in transit	TLS 1.2 or higher for all browser and API communications
Access control	Role-based access controls by user, group, cabinet, document type, function, and workflow role
Identity integration	Microsoft Entra ID single sign-on via OIDC against Customer's tenant; MFA enforced through Customer's identity provider
Deprovisioning	Access revoked within minutes of removal from the applicable Entra ID group
Audit logging	Tamper-evident logging of user access, document activity, search queries, workflow actions, approvals, metadata changes, redactions, deletions, and failed authentication, each with user identity, timestamp, IP address, and action detail. Exportable via self-service tools (Agreement, Section 5.9)
Redaction	Permanent data-level redaction; content destroyed at the data level, not visually masked; original preserved in a permission-locked copy; all actions logged
Tenant isolation	Logical separation of customer tenants and customer data
Environments	Separate Production and UAT environments (Agreement, Section 2.4)
Monitoring	24×7 application and infrastructure monitoring for availability, performance, capacity, and security events
Incident response	Documented procedure covering detection, containment, notification, documentation, and recovery
Vulnerability management	Security patches applied per severity assessment; standard updates during maintenance windows; UAT validation before Production promotion

4. CERTIFICATIONS

Credential	Detail
SOC 2 Type II	Security and Availability trust services criteria, covering EasyFile document imaging and ECM systems. Independent third-party audit conducted annually. Subservice organization: Microsoft Azure (carve-out method). See Agreement, Section 6.2
Azure FedRAMP High	Infrastructure layer authorization held by Microsoft Azure
Azure certifications	Azure holds SOC 1/2/3, ISO 27001, and ISO 27017/27018 covering the infrastructure layer

5. SUBPROCESSORS

The following third parties process Customer Data on CASO's behalf in delivering the Subscription Service. Changes to this list are governed by **Agreement, Section 5.8**, which provides thirty (30) days' advance notice and a right to object.

Subprocessor	Purpose	Type
Microsoft Azure	Cloud hosting, storage, database, networking, and infrastructure	Core
Azure AI Document Intelligence	OCR, text extraction, and layout analysis for capture, extraction, and indexing	Core
AI Provider	Foundation model inferencing for enabled AI features. Applies under the CASO-Managed Model; see Schedule B	Optional — only if AI Services are enabled

5.1 Embedded Components. Apryse document viewing, annotation, and redaction components are embedded in EasyFile and licensed by CASO. These components execute within the Subscription Service and do not receive Customer Data as an independent processor.

5.2 Customer-Controlled Integrations. The Subscription Service integrates with third-party services under Customer's own accounts, including Microsoft Entra ID, Microsoft 365 and Exchange Online,

DocuSign, and Microsoft Power BI. These are not CASO subprocessors. The agreement between Customer and each provider governs that provider's data handling. CASO is responsible for its own processing of Customer Data within EasyFile and for transmissions CASO performs in delivering a configured integration.

6. INTEGRATION AND API SECURITY

Area	Practice
API authentication	OAuth2 bearer tokens or API key authentication required on every request; scoped tokens
API transport	TLS 1.2 or higher
API logging	All API access logged
Rate limiting	Applied to protect service integrity
Webhook validation	DocuSign Listener uses real-time HMAC-SHA256 validation
API stability	Backward compatibility maintained; 90 days' advance notice of breaking changes with migration guides (Agreement, Section 2.7)

7. SECURITY REVIEW PACKAGE

On written request and subject to confidentiality obligations, CASO will provide a security review package including SOC 2 Type II report access, an infrastructure summary, a data flow overview, the subprocessor list, an incident response summary, and standard security questionnaire responses (Agreement, Section 6.5).

8. INCIDENT RESPONSE

CASO maintains a documented incident response procedure covering detection, containment, notification, documentation, and recovery.

Customer is notified within twenty-four (24) hours of a confirmed Security Incident, with the information described in **Agreement, Section 6.4**. Operational incident notification for Severity 1 and Severity 2 events is governed by **Schedule A, Section 5.3**.

9. CHANGES TO THIS SCHEDULE

CASO may update this Schedule to reflect operational changes, **provided no update materially reduces the level of protection for Customer Data during the Subscription Term** and subprocessor changes follow Agreement, Section 5.8. Changes that reduce a stated commitment require a written amendment signed by both parties.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

CASO DOCUMENT MANAGEMENT, INC

COMPREHENSIVE SOFTWARE SOLUTIONS FOR DOCUMENT SCANNING, ELECTRONIC
DOCUMENT MANAGEMENT, AND CONTRACT LIFE CYCLE MANAGEMENT

EXHIBIT N - EASYFILE® ORDER FORM

TO BE COMPLETED WITH KERN

This Order Form is entered into under, and incorporates, the EasyFile Master Subscription Agreement between the parties and its Schedules A, B, and C.

1. PARTIES

Provider	CASO Document Management, Inc., a New York corporation
Provider address	134 West 29th Street, 11th Floor, New York, NY 10001
Customer	Kern County Behavioral Health & Recovery Services
Customer address	2001 28th Street, Bakersfield, CA 93301

2. TERM

Subscription Term	Five (5) years
Start date	_____
End date	_____

3. SUBSCRIPTION

Tier	EasyFile Automation
Authorized Users	300 named users

3.1 Modules and components included. The following are included in the subscription fee at no additional per-module, per-feature, or per-transaction charge:

Core platform	EasyFile EDM
Clients	EasyFileX web client · EFDesktop Windows client
Capture and workflow	EasyFile Capture · ECMToolbox Workflow · Smart Forms
Email and productivity	Mailbox Downloader · EFConnector for Outlook · Virtual Print Driver
Integrations	Microsoft Entra ID SSO · DocuSign Listener · Power BI data connector
Developer	EasyFile REST API, with documentation, code samples, SDKs, and Postman collection
AI	EasyFile AI Connector — subject to Schedule B and Section 7 below

3.2 Environments. Production and User Acceptance Testing.

4. FEES

4.1 Subscription fees. Fixed for the Subscription Term. No CPI, index, or inflation escalation applies.

Year 1	Year 2	Year 3	Year 4	Year 5	Five-year total
\$80,000	\$80,000	\$80,000	\$80,000	\$80,000	\$400,000

4.2 Professional Services. One-time fixed fee of **\$530,000**. No time-and-materials charges apply. Professional Services cover discovery and requirements validation, system configuration and cabinet architecture, contract lifecycle management build, capture and automation build, integration work, digital content migration, training delivery, and project management. Scope, deliverables, milestones, and payment schedule are governed by the statement of work between the parties.

4.3 Not included. The following require a signed change order: Contract Monitoring Tool integration by REST API where integration rather than replacement is selected; Workday (Kern 360) bi-directional integration; Capture AI model expansion beyond the workflows scoped in CASO's proposal; digital content migration materially exceeding 900 GB; dashboards beyond the standard set; user licenses above the number stated in Section 3.

4.4 Optional services. Available at Customer's election by amended Order Form.

Option	Price
Custom Power BI dashboard	\$2,500 each

Power BI training	\$1,500 per half-day session
Extended support — evenings to 10:00 PM Pacific, Monday–Friday	\$6,000 per year
Extended support — Saturday 9:00 AM – 5:00 PM Pacific	\$8,000 per year
24x7 emergency coverage — Severity 1 response	\$15,000 per year

5. CUSTOMER-SPECIFIC TERMS

5.1 Business Hours. Notwithstanding Schedule A, Section 1.2, Business Hours for this Customer are **Monday through Friday, 8:00 AM to 6:00 PM Pacific Time**, excluding holidays observed by Customer.

6. CONTACTS

6.1 CASO.

Role	Name	Contact
Project Manager	Adam Fisk	_____
Project Manager, West Coast	Candice Vance	_____
Technical Lead — escalation	Bill Cross	_____
Executive escalation	Richard Tamaro, President & Chief Executive Officer	_____

6.2 Customer.

Role	Name	Contact
Project Sponsor	_____	_____
IT Lead	_____	_____
EasyFile Administrator	_____	_____
EasyFile Administrator	_____	_____
Notices	Gail Eckels, Administrative Coordinator	GEckels@kernbhrs.org

6.3 After-hours contacts. Outside Business Hours, Customer may contact the individuals listed below. This is provided as a courtesy and does not alter the support commitments in Schedule A.

Name	Contact

7. AI SERVICES ELECTION

AI Services are delivered under either deployment model described in Schedule B and are not activated in Production until Customer authorizes activation in writing.

Deployment model — Customer elects one:

- ☐ **BYOK** — Customer provides and controls the AI Provider account, endpoint, and credentials. Customer pays its provider directly. No CASO surcharge applies.
- ☐ **CASO-Managed** — CASO provides access under its own account. Usage is billed at actual cost plus a fifteen percent (15%) administrative fee.

8. DOCUMENTS

This Order Form incorporates the following:

EasyFile Master Subscription Agreement
Schedule A — Service Levels, Support, and Recovery
Schedule B — AI Services Addendum
Schedule C — Security and Compliance Summary

9. SIGNATURES

By signing below, each party agrees to this Order Form and the documents incorporated in Section 8.

CASO DOCUMENT MANAGEMENT, INC.

Signature	
Name	Richard Tamaro
Title	President & Chief Executive Officer
Date	

KERN COUNTY BEHAVIORAL HEALTH & RECOVERY SERVICES

Signature
Name
Title
Date

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

[END OF THE AGREEMENT]