FRAMEWORK AGREEMENT

THIS FRAMEWORK AGREEMENT is made between the **CITY AND COUNTY OF DENVER**, a municipal corporation of the State of Colorado (the "City"), and **NAPHCARE, INC,** a Alabama corporation, whose address is 2090 Columbiana Rd Ste 4000, Vestavia Hills, AL 35216 (the "Contractor"), individually a "Party" and jointly "the Parties."

RECITALS

WHEREAS, the City awarded this Agreement to the Contractor through a competitive selection for the purchase of software licensing, implementation, and support for the TechCare Electronic Health Records system (this "Agreement").

NOW, THEREFORE, in consideration of the mutual covenants and agreements hereinafter set forth and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties incorporate the recitals set forth above agree as follows:

1. **COORDINATION AND LIAISON**: The Contractor shall fully coordinate all Work under this Agreement with the City's Chief Information Officer ("CIO") or other designated personnel of the Department of Technology Services ("Agency" or "TS").
2. **DEFINITIONS**
   - **2.1.** "**City Data**" means all information processed or stored on computers or other electronic media by the City or on the City's behalf or provided to the Contractor for such processing or storage, as well as any information derived from such information. City Data includes, without limitation: (i) information on paper or other non-electronic media provided to the Contractor for computer processing or storage, or information formerly on electronic media; (ii) information provided to the Contractor by the City, other users, or by other third parties; and (iii) personally identifiable information, confidential or sensitive information, or other regulated data from such users or other third parties, including from the City's employees.
   - **2.2.** "**D(d)ata**" means information, regardless of form, that can be read, transmitted, or processed.
   - **2.3.** "**Deliverable(s)**" means a tangible object, SaaS, or On-Premise Software that is provided to the City by the Contractor under this Agreement.
   - **2.4.** "**Effective Date**" means the date on which this Agreement is approved and signed by the City as shown on the City's signature page.
   - **2.5.** "**Exhibits**" means the exhibits and attachments included with this Agreement.
   - **2.6.** "**On-Premise Software**" means software that the Contractor provides for the City's use. For the avoidance of doubt, On-Premise Software does not include SaaS, though On-Premise Software may interface with SaaS.
   - **2.7.** "**SaaS**" means a software-as-a-service that the Contractor hosts (directly or indirectly) for the City's use. For the avoidance of doubt, SaaS does not include Services or On-Premise Software.
   - **2.8.** "**Service(s)**" means the technology related professional services to be performed by the Contractor as set forth in this Agreement and shall include any services or support provided by the Contractor under this Agreement.
   - **2.9.** "**Specifications**" refers to such technical and functional specifications for On-Premise Software, SaaS, and/or Deliverables included or referenced in an Exhibit.

2.10. "**Subcontractor**" means any third party engaged by the Contractor to aid in performance of the Work.

2.11. "**Task Order**" means a document issued in accordance with this Agreement that specifically describes the Work to be performed.

2.12. "**Work**" means the On-Premise Software, SaaS, Services, hardware, or Deliverables provided and/or performed pursuant to this Agreement.

3. SOFTWARE AS A SERVICE, SUPPORT, AND SERVICES TO BE PERFORMED: As the City directs, the Contractor shall diligently undertake, perform, and make available the technology related Work set forth in the Exhibits to the City's satisfaction. The City shall have no liability to compensate the Contractor for Work that is not specifically authorized by this Agreement. The Work shall be provided and performed as stated herein and shall conform to the Specifications. The Contractor is ready, willing, and able to provide the Work required by this Agreement. The Contractor shall faithfully perform any Services in accordance with the standards of care, skill, training, diligence, and judgment provided by highly competent individuals performing services of a similar nature to those described in this Agreement and in accordance with the terms of this Agreement.

4. TASK ORDERS FOR ADDITIONAL PRODUCTS AND SERVICES

4.1. To initiate a Task Order, the City will provide a request to the Contractor describing the general scope and intent of the Work it desires the Contractor to perform under that Task Order. The Contractor shall submit a proposal, which shall include a quote, to the City in response to the City's request. All Task Orders, signed by the Parties, shall be issued in accordance with this Agreement using the rates contained therein. Each Task Order shall include a detailed scope of Services, level of effort, timeline for completion, rates or fixed fee pricing, and payment schedule, including a "not to exceed" amount, specific to each Task Order. Task Orders shall be construed to be in addition to, supplementary to, and consistent with the provisions of this Agreement. In the event of a conflict between a particular provision of any Task Order and a provision of this Agreement, this Agreement shall take precedence. A Task Order may be amended by the Parties by a written instrument prepared by the Parties jointly and signed by their authorized representatives.

4.2. The City is not required to execute any minimum number of Task Orders under this Agreement, and the City reserves the right to execute Task Orders with the Contractor at its sole discretion. The City shall have no liability to compensate the Contractor for any Work not specifically set forth in this Agreement or a properly executed Task Order. In no event shall a Task Order term extend beyond the Term unless the City has specifically agreed in writing. If this Agreement is terminated for any reason, each Task Order hereunder shall also terminate unless the City has specifically directed otherwise in writing. Task Orders may also be terminated in accordance with this Agreement's termination provisions. The Contractor agrees to fully coordinate its provision of Services with any third party under contract with the City doing work or providing Services which affect the Contractor's performance.

4.3. The Contractor represents and warrants that all Services under a Task Order will be performed by qualified personnel in a professional and workmanlike manner, consistent with industry standards; all Services and/or Deliverables will conform to applicable, agreed upon specifications, if any;

and, it has the requisite ownership, rights and licenses to perform its obligations under this Agreement fully as contemplated hereby and to grant to the City all rights with respect to any software and Services free and clear from any and all liens, adverse claims, encumbrances and interests of any third party.

5. **TERM**: This Agreement will commence on December 1, 2024, and will expire, unless sooner terminated, on August 1, 2030 (the "Term"). Subject to the City's prior written authorization, the Contractor shall complete any work in progress as of the expiration date and the Term will extend until the work is completed or earlier terminated by the City.
6. **END OF TERM EXTENSION**: If this Agreement approaches the end of its Term, the City, at its discretion and upon written notice to the Contractor as provided herein, may unilaterally extend the Term for a period not to exceed six months (an "End of Term Extension). The provisions of this Agreement and the pricing in effect when such notice is given shall remain in effect during the End of Term Extension. The End of Term Extension shall automatically terminate upon execution of a replacement contract or modification extending this Agreement. To facilitate any agreed upon extensions in a timely manner, the Contractor shall negotiate any extension of this Agreement in good faith and provide the City all required order forms and updated pricing information to the City no later than 120 days prior to the expiration of the Term. If the Contractor does not intend to extend the Term of this Agreement, the Contractor shall provide prompt notice to the City but not later than one hundred (180) days prior to the expiration of the Term of its intent to let this Agreement lapse without an extension or replacement contract. The Contractor's obligation to facilitate a timely renewal under this Section is a material part of this Agreement.
7. **COMPENSATION AND PAYMENT**
   - **7.1. Fees**: The City shall pay, and the Contractor shall accept as the sole compensation for Services rendered and costs incurred under this Agreement the fees described in the attached Exhibits. Amounts billed may not exceed rates set forth in the Exhibits and will be made in accordance with any agreed upon payment milestones.
   - **7.2. Reimbursement Expenses**: There are no reimbursable expenses allowed under this Agreement. All the Contractor's expenses are contained in the budget as described in the Exhibits. The City will not be obligated to pay the Contractor for any other fees, costs, expenses, or charges of any nature that may be incurred and paid by the Contractor in performing their obligations under this Agreement including but not limited to personnel costs, benefits, contract labor, overhead, administrative costs, operating costs, supplies, equipment, and out-of-pocket expenses.
   - **7.3. Invoicing**: The Contractor must submit an invoice which shall include the City contract number, clear identification of the Work that has been completed or delivered, and other information reasonably requested by the City. Payment on all uncontested amounts shall be made in accordance with the City's Prompt Payment Ordinance, §§ 20-107, *et seq.*, D.R.M.C, and no Exhibit or order form shall modify the City's statutory payment provisions.
   - **7.4. Maximum Contract Amount**
     - **7.4.1.** Notwithstanding any other provision of this Agreement, the City's maximum payment obligation will not exceed One Million Eight Hundred Forty-One Thousand Nine Hundred

Seventy-Eight Dollars ($1,841,978.00) (the "Maximum Agreement Amount"). The City is not obligated to execute an Agreement or any amendments for any further Work, including any Services performed by the Contractor beyond that specifically described in the attached Exhibits. Any Work performed beyond those in the attached Exhibits are performed at the Contractor's risk and without authorization under this Agreement.

7.4.2. The City's payment obligation, whether direct or contingent, extends only to funds appropriated annually by the Denver City Council, paid into the Treasury of the City, and encumbered for the purpose of this Agreement. The City does not by this Agreement irrevocably pledge present cash reserves for payment or performance in future fiscal years. This Agreement does not and is not intended to create a multiple-fiscal year direct or indirect debt or financial obligation of the City.

8. TAXES, CHARGES AND PENALTIES: The City shall not be liable for the payment of taxes, late charges, or penalties of any nature other than the compensation stated herein, except for any additional amounts which the City may be required to pay under D.R.M.C. § 20-107 to § 20-115.

9. STATUS OF CONTRACTOR: The Contractor is an independent contractor retained to perform professional or technical services for limited periods of time. Neither the Contractor nor any of its employees are employees or officers of the City under Chapter 18 of the Denver Revised Municipal Code, or for any purpose whatsoever. Nothing contained in this Agreement shall be construed as creating any agency, partnership, joint venture, or other form of joint enterprise, or employment relationship between the Parties.

10. TERMINATION

10.1. Either Party may terminate this Agreement, and the City may terminate a product under this Agreement, for the other Party's material breach by written notice specifying in detail the nature of the breach, effective in thirty (30) days unless the other Party first cures such breach, or effective immediately if the breach is not subject to cure.

10.2. The City has the right to terminate this Agreement or a product under this Agreement without cause upon thirty (30) days prior written notice to the Contractor. The Contractor has the right to terminate this Agreement without cause upon three hundred sixty (360) days prior written notice to the City. Nothing gives the Contractor the right to perform under this Agreement beyond the time when its Work becomes unsatisfactory to the City. Notwithstanding anything to the contrary contained in this Agreement, if the City terminates this Agreement without cause, the City shall be under no obligation to make further payment(s) for any remaining subscription years, licensing fees, or support costs as outlined in the attached Exhibits once the then current annual term expires; provide that, the City shall not be entitled to any refund, unless stated otherwise in the Exhibits, for the remainder of the prepaid annual term then in effect at the time of this Agreement's early termination without cause.

10.3. Notwithstanding the preceding paragraph, the City may terminate this Agreement if the Contractor or any of its officers or employees are convicted, plead nolo contendere, enter into a formal agreement in which they admit guilt, enter a plea of guilty or otherwise admit culpability to criminal offenses of bribery, kickbacks, collusive bidding, bid-rigging, antitrust, fraud, undue

influence, theft, racketeering, extortion or any offense of a similar nature in connection with the Contractor's business. Termination for the reasons stated in this paragraph is effective upon receipt of notice.

10.4. Upon termination of this Agreement, with or without cause, the Contractor shall have no claim against the City by reason of, or arising out of, incidental or relating to termination, except for compensation for work duly requested and satisfactorily performed. Upon The City's request or upon termination, the Contractor shall return to the City all property placed in the Contractor's possession or control pursuant to this Agreement.

10.5. The City is entering into this Agreement to serve the public interest of the City as determined by its governing bodies. If this Agreement ceases to further the public interest of the City, or if the City fails to appropriate the necessary funding to continue this Agreement, the City, in its discretion, may terminate this Agreement in whole or in part. A determination that this Agreement should be terminated in the public interest or for lack of appropriation shall not be equivalent to a City right to terminate for convenience or without cause. This Subsection shall not apply to a termination of this Agreement by the City for a breach of contract by the Contractor. If the City terminates this Agreement in the public interest or for lack of appropriation, the City shall pay the Contractor an amount equal to the percentage of the total reimbursement payable under this Agreement that corresponds to the percentage of Work satisfactorily delivered or completed and accepted, as determined by the City, less payments previously made.

11. **EXAMINATION OF RECORDS AND AUDITS**: Any authorized agent of the City, including the City Auditor or his or her representative, has the right to access, and the right to examine, copy and retain copies, at City's election in paper or electronic form, any pertinent books, documents, papers and records related to the Contractor's performance pursuant to this Agreement, provision of any goods or services to the City, and any other transactions related to this Agreement. The Contractor shall cooperate with City representatives and City representatives shall be granted access to the foregoing documents and information during reasonable business hours and until the latter of three (3) years after the final payment under this Agreement or expiration of the applicable statute of limitations. When conducting an audit of this Agreement, the City Auditor shall be subject to government auditing standards issued by the United States Government Accountability Office by the Comptroller General of the United States, including with respect to disclosure of information acquired during the course of an audit. No examination of records and audits pursuant to this paragraph shall require the Contractor to make disclosures in violation of state or federal privacy laws. The Contractor shall at all times comply with D.R.M.C. 20-276.

12. **WHEN RIGHTS AND REMEDIES NOT WAIVED**: In no event shall any action by either Party hereunder constitute or be construed to be a waiver by the other Party of any breach of covenant or default which may then exist on the part of the Party alleged to be in breach, and the non-breaching Party's action or inaction when any such breach or default shall exist shall not impair or prejudice any right or remedy available to that Party with respect to such breach or default; and no assent, expressed or implied, to any breach of any one or more covenants, provisions or conditions of this Agreement shall be deemed or taken to be a waiver of any other breach.

13. INSURANCE

13.1. **General Conditions**: The Contractor agrees to secure, at or before the time of execution of this Agreement, the following insurance covering all operations, goods or services provided pursuant to this Agreement. The Contractor shall keep the required insurance coverage in force at all times during the term of this Agreement, including any extension thereof, and during any warranty period. The required insurance shall be underwritten by an insurer licensed or authorized to do business in Colorado and rated by A.M. Best Company as "A-VIII" or better. Each policy shall require notification to the City in the event any of the required policies be canceled or non-renewed before the expiration date thereof. Such written notice shall be sent to the parties identified in the Notices Section of this Agreement. Such notice shall reference the City contract number listed on the signature page of this Agreement. Said notice shall be sent thirty (30) days prior to such cancellation or non-renewal unless due to non-payment of premiums for which notice shall be sent ten (10) days prior. If such written notice is unavailable from the insurer, the Contractor shall provide written notice of cancellation, non-renewal and any reduction in coverage to the parties identified in the Notices Section by certified mail, return receipt requested within three (3) business days of such notice by its insurer(s) and referencing the City's contract number. The Contractor shall be responsible for the payment of any deductible or self-insured retention. The insurance coverages specified in this Agreement are the minimum requirements, and these requirements do not lessen or limit the liability of the Contractor. The Contractor shall maintain, at its own expense, any additional kinds or amounts of insurance that it may deem necessary to cover its obligations and liabilities under this Agreement.

13.2. **Proof of Insurance**: The Contractor may not commence services or work relating to this Agreement prior to placement of coverages required under this Agreement. The Contractor certifies that the certificate of insurance attached as **Exhibit D**, preferably an ACORD form, complies with all insurance requirements of this Agreement. The City requests that the City's contract number be referenced on the certificate of insurance. The City's acceptance of a certificate of insurance or other proof of insurance that does not comply with all insurance requirements set forth in this Agreement shall not act as a waiver of the Contractor's breach of this Agreement or of any of the City's rights or remedies under this Agreement. The City's Risk Management Office may require additional proof of insurance, including but not limited to policies and endorsements.

13.3. **Additional Insureds**: For Commercial General Liability, Auto Liability and Excess Liability/Umbrella (if required), the Contractor and Subcontractor's insurer(s) shall include the City and County of Denver, its elected and appointed officials, employees, and volunteers as additional insured.

13.4. **Waiver of Subrogation**: For all coverages required under this Agreement, with the exception of Professional Liability – if required, the Contractor's insurer shall waive subrogation rights against the City.

13.5. **Subcontractors and Subconsultants**: The Contractor shall confirm and document that all Subcontractors and subconsultants (including independent contractors, suppliers or other entities

providing goods or services required by this Agreement) procure and maintain coverage as approved by the Contractor and appropriate to their respective primary business risks considering the nature and scope of services provided.

13.6. **Workers' Compensation and Employer's Liability Insurance**: The Contractor shall maintain the coverage as required by statute for each work location and shall maintain Employer's Liability insurance with limits of $100,000 per occurrence for each bodily injury claim, $100,000 per occurrence for each bodily injury caused by disease claim, and $500,000 aggregate for all bodily injuries caused by disease claims.

13.7. **Commercial General Liability**: The Contractor shall maintain a Commercial General Liability insurance policy with minimum limits of $1,000,000 for each bodily injury and property damage occurrence, $2,000,000 products and completed operations aggregate (if applicable), and $2,000,000 policy aggregate.

13.8. **Automobile Liability**: The Contractor shall maintain Automobile Liability with minimum limits of $1,000,000 combined single limit applicable to all owned, hired, and non-owned vehicles used in performing services under this Agreement.

13.9. **Cyber Liability**: The Contractor shall maintain Cyber Liability coverage with minimum limits of $1,000,000 per occurrence and $1,000,000 policy aggregate covering claims involving privacy violations, information theft, damage to or destruction of electronic information, intentional and/or unintentional release of private information, alteration of electronic information, extortion and network security. If Claims Made, the policy shall be kept in force, or a Tail policy placed, for three (3) years.

13.10. **Technology Errors & Omissions**: The Contractor shall maintain Technology Errors and Omissions insurance including network security, privacy liability and product failure coverage with minimum limits of $1,000,000 per occurrence and $1,000,000 policy aggregate. The policy shall be kept in force, or a Tail policy placed, for three (3) years.

14. DEFENSE AND INDEMNIFICATION

14.1. The Contractor hereby agrees to defend, indemnify, reimburse and hold harmless City, its appointed and elected officials, agents and employees for, from and against all liabilities, claims, judgments, suits or demands for damages to persons or property arising out of, resulting from, or relating to the work performed under this Agreement ("Claims"), unless such Claims have been specifically determined by the trier of fact to be the sole negligence or willful misconduct of the City. This indemnity shall be interpreted in the broadest possible manner to indemnify City for any acts or omissions of the Contractor or its Subcontractors either passive or active, irrespective of fault, including City's concurrent negligence whether active or passive, except for the sole negligence or willful misconduct of City.

14.2. The Contractor's duty to defend and indemnify City shall arise at the time written notice of the Claim is first provided to City regardless of whether Claimant has filed suit on the Claim. the Contractor's duty to defend and indemnify City shall arise even if City is the only party sued by claimant and/or claimant alleges that City's negligence or willful misconduct was the sole cause of claimant's damages.

14.3. The Contractor will defend any and all Claims which may be brought or threatened against City and will pay on behalf of City any expenses incurred by reason of such Claims including, but not limited to, court costs and attorney fees incurred in defending and investigating such Claims or seeking to enforce this indemnity obligation. Such payments on behalf of City shall be in addition to any other legal remedies available to City and shall not be considered City's exclusive remedy.

14.4. Insurance coverage requirements specified in this Agreement shall in no way lessen or limit the liability of the Contractor under the terms of this indemnification obligation. The Contractor shall obtain, at its own expense, any additional insurance that it deems necessary for the City's protection.

14.5. The Contractor shall indemnify, save, and hold harmless the indemnified parties, against any and all costs, expenses, claims, damages, liabilities, and other amounts (including attorneys' fees and costs) incurred by the indemnified parties in relation to any claim that any Work provided by the Contractor under this Agreement (collectively, "IP Deliverables"), or the use thereof, infringes a patent, copyright, trademark, trade secret, or any other intellectual property right. The Contractor's obligations hereunder shall not extend to the combination of any IP Deliverables provided by the Contractor with any other product, system, or method, unless the other product, system, or method is (i) provided by the Contractor or the Contractor's subsidiaries or affiliates; (ii) specified by the Contractor to work with the IP Deliverables; (iii) reasonably required in order to use the IP Deliverables in its intended manner and the infringement could not have been avoided by substituting another reasonably available product, system, or method capable of performing the same function; or (iv) is reasonably expected to be used in combination with the IP Deliverables.

14.6. The Contractor shall indemnify, save, and hold harmless the indemnified parties against all costs, expenses, claims, damages, liabilities, court awards and other amounts, including attorneys' fees and related costs, incurred by the indemnified parties in relation to the Contractor's failure to comply with §§ 24-85-101, *et seq.*, C.R.S., or the *Accessibility Standards for Individuals with a Disability* as established pursuant to § 24-85-103 (2.5), C.R.S. This indemnification obligation does not extend to the City's generated content using the Contractor's software, including any configuration or customization of the Contractor's software by the City.

14.7. This defense and indemnification obligation shall survive the expiration or termination of this Agreement.

15. LIMITATION OF THE CONTRACTOR'S LIABILITY: To the extent permitted by law, the liability of the Contractor, its Subcontractors, and their respective personnel to the City for any claims, liabilities, or damages relating to this Agreement shall be limited to damages, including but not limited to direct losses, consequential, special, indirect, incidental, punitive or exemplary loss, loss or unauthorized disclosure of City Data, not to exceed three (3) times the Maximum Agreement Amount payable by the City under this Agreement. No limitation on the Contractor's liability to the City under this Section shall limit or affect: (i) the Contractor's indemnification obligations to the City under this Agreement; (ii) any claims, losses, or damages for which coverage is available under any insurance

required under this Agreement; (iii) claims or damages arising out of bodily injury, including death, or damage to tangible property of the City; or (iv) claims or damages resulting from the recklessness, bad faith, or intentional misconduct of the Contractor or its Subcontractors.

16. **COLORADO GOVERNMENTAL IMMUNITY ACT**: The Parties hereto understand and agree that the City is relying upon, and has not waived, the monetary limitations and all other rights, immunities and protection provided by the Colorado Governmental Act, § 24-10-101, *et seq*., C.R.S.
17. **COMPLIANCE WITH APPLICABLE LAWS AND POLICIES**: The Contractor shall comply with all applicable laws, rules, regulations and codes of the United States, the State of Colorado; and with the Charter, ordinances, rules, regulations, public health orders, and Executive Orders of the City and County of Denver that are applicable to the Contractor's performance hereunder. These laws, regulations, and other authorities are incorporated by reference herein to the extent that they are applicable. Any of the Contractor's personnel visiting the City's facilities will comply with all applicable City policies regarding access to, use of, and conduct within such facilities. The City will provide copies of such policies to the Contractor upon request.
18. **COMPLIANCE WITH DENVER WAGE LAWS**: To the extent applicable to the Contractor's provision of Services hereunder, the Contractor shall comply with, and agrees to be bound by, all rules, regulations, requirements, conditions, and City determinations regarding the City's Minimum Wage and Civil Wage Theft Ordinances, Sections 58-1 through 58-26 D.R.M.C., including, but not limited to, the requirement that every covered worker shall be paid all earned wages under applicable state, federal, and city law in accordance with the foregoing D.R.M.C. Sections. By executing this Agreement, the Contractor expressly acknowledges that the Contractor is aware of the requirements of the City's Minimum Wage and Civil Wage Theft Ordinances and that any failure by the Contractor, or any other individual or entity acting subject to this Agreement, to strictly comply with the foregoing D.R.M.C. Sections shall result in the penalties and other remedies authorized therein.
19. **DATA PROTECTION**: The Contractor recognizes and agrees that: (i) City Data is valuable property of the City; (ii) City Data may include Confidential Information, protected or regulated data, and trade secrets of the City; and (iii) the City has dedicated substantial resources to collecting, managing, protecting, and compiling City Data. The Contractor recognizes and agrees that City Data may contain personally identifiable information or other sensitive information, even if the presence of such information is not labeled or disclosed. If the Contractor receives access to City Data, the Contractor shall comply with all applicable data protection laws, including the Colorado Consumer Protection Act and the Colorado Privacy Act, to the extent applicable. Other such obligations may arise from the Health Information Portability and Accountability Act (HIPAA), IRS Publication 1075, Payment Card Industry Data Security Standard (PCI-DSS), and the FBI Criminal Justice Information Service Security Addendum. At a minimum, the Contractor shall implement and maintain all appropriate administrative, physical, technical, and procedural safeguards necessary and appropriate to ensure compliance with the standards and guidelines applicable to the Contractor's performance under this Agreement. The Contractor shall also comply with the terms and conditions in the attached **Exhibit E**, Information Technology Provisions. Any Exhibit or external term hereto may not waive or modify

the Contractor's legal obligations to protect City Data in compliance with applicable law under this Agreement.

20. **SAFEGUARDING PERSONAL INFORMATION**: "PII" means personally identifiable information including, without limitation, any information maintained by the City about an individual that can be used to distinguish or trace an individual's identity, including, but not limited to, first and last name, residence or other physical address, banking information, electronic mail address, telephone number, credit card information, an official government-issued driver's license or identification card number, social security number or tax identification number, date and place of birth, mother's maiden name, or biometric records. PII includes, but is not limited to, all information defined as personally identifiable information in §§ 24-73-101, C.R.S. "PII" shall also include "personal information" as defined in § 24-73-103(1)(g), C.R.S. If the Contractor or any of its Subcontractors receives PII under this Agreement, the Contractor shall provide for the security of such PII, in a manner and form acceptable to the City, including, without limitation, non-disclosure requirements, use of appropriate technology, security practices, computer and data access security, data storage and transmission encryption, security inspections, and audits. As applicable, the Contractor shall be a "Third-Party Service Provider" as defined in § 24-73-103(1)(i), C.R.S., and shall maintain security procedures and practices consistent with §§ 24-73-101, *et seq.*, C.R.S. In addition, as set forth in § 28-251, D.R.M.C., the Contractor, including, but not limited to, the Contractor's employees, agents, and Subcontractors, shall not collect or disseminate individually identifiable information about the national origin, immigration, or citizenship status of any person, over and above the extent to which the City is required to collect or disseminate such information in accordance with any federal, state, or local law.

21. **SECURITY BREACH AND REMEDIATION**

    21.1. **Security Breach**: If the Contractor becomes aware of a suspected or unauthorized acquisition or disclosure of unencrypted data, in any form, that compromises the security, access, confidentiality, or integrity of City Data (a "Security Breach"), the Contractor shall notify the City in the most expedient time and without unreasonable delay. A Security Breach shall also include, without limitation, (i) attempts to gain unauthorized access to a City system or City Data regardless of where such information is located; (ii) unwanted disruption or denial of service; (iii) the unauthorized use of a City system for the processing or storage of data; or (iv) changes to the City's system hardware, firmware, or software characteristics without the City's knowledge, instruction, or consent. Any oral notice of a Security Breach provided by the Contractor shall be immediately followed by a written notice to the City.

    21.2. **Remediation**: The Contractor shall implement and maintain a program for managing actual or suspected Security Breaches. In the event of a Security Breach, the Contractor shall cooperate with the City and law enforcement agencies, when applicable, to investigate and resolve the Security Breach, including, without limitation, providing reasonable assistance to the City in notifying third parties. The Contractor shall provide the City prompt access to such records related to a Security Breach as the City may reasonably request; provided such records will be the Contractor's Confidential Information, and the Contractor will not be required to provide the City with records belonging to, or compromising the security of, its other customers. The provisions

of this Subsection do not limit the City's other rights or remedies, if any, resulting from a Security Breach. In addition, unless the Security Breach resulted from the City's sole act or omission, the Contractor shall promptly reimburse the City for reasonable costs incurred by the City in any investigation, remediation or litigation resulting from any Security Breach, including but not limited to providing notification to third parties whose data was compromised and to regulatory bodies, law-enforcement agencies, or other entities as required by law or contract; establishing and monitoring call center(s), and credit monitoring and/or identity restoration services to assist each person impacted by a Security Breach in such a fashion that, in the City's sole discretion, could lead to identity theft; and the payment of reasonable legal fees and expenses, audit costs, fines and penalties, and other fees imposed by regulatory agencies, courts of law, or contracting partners as a result of the Security Breach attributable to the Contractor or its Subcontractors.

22. ACCESSIBILITY AND ADA WEBSITE COMPLIANCE

22.1. **Compliance**: The Contractor shall comply with, and the Work provided under this Agreement shall be in compliance with, all applicable provisions of §§ 24-85-101, *et seq.*, C.R.S., and the *Accessibility Standards for Individuals with a Disability*, as established pursuant to Section § 24-85-103 (2.5), C.R.S. (collectively, the "Guidelines"), to the extent required by law. The Contractor shall also comply with Level AA of the most current version of the Web Content Accessibility Guidelines (WCAG), incorporated in the State of Colorado technology standards.

22.2. **Testing**: The City may require the Contractor's compliance to be determined by a third party selected by the City to attest that the Contractor's has performed all obligations under this Agreement in compliance with §§ 24-85-101, *et seq.*, C.R.S., and the Accessibility Standards for Individuals with a Disability as established pursuant to § 24-85-103 (2.5), C.R.S.

22.3. **Validation and Remediation**: The Contractor agrees to promptly respond to and resolve any instance of noncompliance regarding accessibility in a timely manner and shall remedy any noncompliant Work at no additional cost to the City. If the City reasonably determines accessibility issues exist, the Contractor shall provide a "roadmap" for remedying those deficiencies on a reasonable timeline to be approved by the City. Resolution of reported accessibility issue(s) that may arise shall be addressed as high priority, and failure to make satisfactory progress towards compliance with the Guidelines, as agreed to in the roadmap, shall constitute a breach of contract and be grounds for termination or non-renewal of this Agreement.

23. CONFIDENTIAL INFORMATION

23.1. "Confidential Information" means all information or data, regardless of form, not subject to disclosure under the Colorado Open Records Act, §§ 24-72-201, *et seq.*, C.R.S. ("CORA"), and is marked or identified at the time of disclosure as being confidential, proprietary, or its equivalent. Each of the Parties may disclose (a "Disclosing Party") or permit the other Party (the "Receiving Party") access to the Disclosing Party's Confidential Information in accordance with the following terms. Except as specifically permitted in this Agreement or with the prior express written permission of the Disclosing Party, the Receiving Party shall not: (i) disclose, allow access to, transmit, transfer or otherwise make available any Confidential Information of the Disclosing Party to any third party other than its employees, Subcontractors, agents and consultants that need

to know such information to fulfill the purposes of this Agreement, and in the case of non-employees, with whom it has executed a non-disclosure or other agreement which limits the use, reproduction and disclosure of the Confidential Information on terms that afford at least as much protection to the Confidential Information as the provisions of this Agreement; or (ii) use or reproduce the Confidential Information of the Disclosing Party for any reason other than as reasonably necessary to fulfill the purposes of this Agreement. This Agreement does not transfer ownership of Confidential Information or grant a license thereto. The City will retain all right, title, and interest in its Confidential Information.

23.2. The Contractor shall provide for the security of Confidential Information and information which may not be marked, but constitutes personally identifiable information or other federally or state regulated information ("Regulated Data") in accordance with all applicable laws and regulations. If the Contractor receives Regulated Data outside the scope of this Agreement, it shall promptly notify the City.

23.3. Disclosed information or data that the Receiving Party can establish: (i) was lawfully in the Receiving Party's possession before receipt from the Disclosing Party; or (ii) is or becomes a matter of public knowledge through no fault of the Receiving Party; or (iii) was independently developed or discovered by the Receiving Party; or (iv) was received from a third party that was not under an obligation of confidentiality, shall not be considered Confidential Information under this Agreement. The Receiving Party will inform necessary employees, officials, Subcontractors, agents, and officers of the confidentiality obligations under this Agreement, and all requirements and obligations of the Receiving Party under this Agreement shall survive the expiration or earlier termination of this Agreement.

23.4. Nothing in this Agreement shall in any way limit the ability of the City to comply with any laws or legal process concerning disclosures by public entities. The Parties understand that all materials exchanged under this Agreement, including Confidential Information, may be subject to CORA. In the event of a request to the City for disclosure of possible confidential materials, the City shall advise the Contractor of such request to give the Contractor the opportunity to object to the disclosure of any of its materials which it marked as, or otherwise asserts is, proprietary or confidential. If the Contractor objects to disclosure of any of its material, the Contractor shall identify to the City the legal basis under CORA for any right to withhold. In the event of any action or the filing of a lawsuit to compel disclosure, the Contractor agrees to intervene in such action or lawsuit to protect and assert its claims of privilege against disclosure of such material or waive the same. If the matter is not resolved, the City will tender all material to the court for judicial determination of the issue of disclosure. The Contractor further agrees to defend, indemnify, and save and hold harmless the City, its officers, agents, and employees, from any claim, damages, expense, attorneys' fees, or costs arising out of the Contractor's intervention to protect and assert its claim of privilege against disclosure under this Section.

24. <u>PROTECTED HEALTH INFORMATION</u>: The Contractor shall comply with all legislative and regulatory requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"); the Health Information Technology for Economic and Clinical Health Act ("HITECH");

42 CFR Part 2, Confidentially of Substance use Disorder Patient Records; the privacy standards adopted by the U.S. Department of Health and Human Services, 45 C.F.R. Parts 160 and 164, Subparts A and E; and the security standards adopted by the U.S. Department of Health and Human Services, 45 C.F.R. Parts 160, 162, 164, and Subpart C (collectively, "HIPAA Rules"). The Contractor shall implement all necessary protective measures to comply with HIPAA Rules, and the Contractor hereby agrees to be bound by the terms of the Business Associate Agreement attached hereto and incorporated herein as **Exhibit F**. The Contractor shall not use protected health information or substance use treatment records except as legally necessary to fulfill the purpose of this Agreement and shall hold the City harmless, to the extent permitted by law, for any breach of these regulations. This Section shall survive the expiration or earlier termination of this Agreement, and the Contractor shall ensure that the requirements of this Section are included in any relevant subcontracts or subgrants.

25. **CRIMINAL JUSTICE INFORMATION**: The Contractor shall comply with all applicable standards of the Criminal Justice Information Services ("CJIS") Security Policy, attached hereto and incorporated herein as **Exhibit G** and all other requirements issued by the Federal Bureau of Investigation ("FBI"). The Contractor shall ensure that any Work provided under this Agreement protects the confidentiality, integrity, and availability of criminal justice information ("CJI") from unauthorized access, use, or disclosure. The Contractor shall ensure its responsibilities related to CJIS compliance are appropriately assigned and maintained and shall cooperate with any audits or inspections conducted by the City, the Colorado Bureau of Investigations, or the FBI to verify compliance with the CJIS Security Policy. The Contractor shall promptly report any breaches or incidents involving CJI to the City and take appropriate remedial actions. Contractors with direct access or indirect access to CJI shall handle all CJI following the CJIS Security Policy and Title 28, Code of Federal Regulations, Part 20 (relevant standards). Contractors supporting systems which provide direct access to CJI shall also follow the regulations listed in the laws, polices, and manuals incorporated into this agreement: NCIC Operating Manual, CCIC Training Manual, Interstate Identification Index / National Fingerprint File Operational and Technical Manual, and Title 28, Code of Federal Regulations, Part 23. Contractors who perform criminal justice functions and have access to CJI shall meet the same training and certification criteria required of governmental agencies performing a similar function and are subject to audit to the same extent as local agencies. Before receiving access to CJI or Federal Criminal History Record Information ("CHRI"), the Contractor and its individual employees must complete the attached CJIS Security Addendum certification attached hereto. The Contractor shall maintain signed CJIS Security Addendum certification pages for its personnel and shall provide copies to the City upon request.

26. **ASSIGNMENT; SUBCONTRACTING**: The Contractor shall not voluntarily or involuntarily assign any of its rights or obligations, or subcontract performance obligations, under this Agreement without obtaining the City's prior written consent. Any assignment or subcontracting without such consent will be ineffective and void and shall be cause for termination of this Agreement by the City. The City has sole and absolute discretion whether to consent to any assignment or subcontracting, or to terminate this Agreement because of unauthorized assignment or subcontracting. The City, at their reasonable discretion, may approve of the assignment or transfer in writing, deny the assignment or

transfer, or refer the matter to the City's governing bodies for approval. In the event of any subcontracting or unauthorized assignment: (i) the Contractor shall remain responsible to the City; and (ii) no contractual relationship shall be created between the City and any subconsultant, Subcontractor, or assign.

27. **NO THIRD-PARTY BENEFICIARY**: Enforcement of the terms of this Agreement and all rights of action relating to enforcement are strictly reserved to the Parties. Nothing contained in this Agreement gives or allows any claim or right of action to any third person or entity. Any person or entity other than the City or the Contractor receiving services or benefits pursuant to this Agreement is an incidental beneficiary only.
28. **NO AUTHORITY TO BIND CITY TO CONTRACTS**: The Contractor lacks any authority to bind the City on any contractual matters. Final approval of all contractual matters that purport to obligate the City must be executed by the City in accordance with the City's Charter and the Denver Revised Municipal Code.
29. **AGREEMENT AS COMPLETE INTEGRATION-AMENDMENTS**: Except for the functional requirements provided in response to a request for proposal and/or any subsequent enhancement of the SOW or other implementation documentation that may be developed after execution of this Agreement, this Agreement is the complete integration of all understandings between the Parties as to the subject matter of this Agreement. No prior, contemporaneous, or subsequent addition, deletion, or other modification has any force or effect, unless embodied in this Agreement in writing. No oral representation by any officer or employee of the City at variance with the terms of this Agreement or any written amendment to this Agreement will have any force or effect or bind the City.
30. **SEVERABILITY**: Except for the provisions of this Agreement requiring appropriation of funds and limiting the total amount payable by the City, if a court of competent jurisdiction finds any provision of this Agreement or any portion of it to be invalid, illegal, or unenforceable, the validity of the remaining portions or provisions will not be affected, if the intent of the Parties can be fulfilled.
31. **CONFLICT OF INTEREST**: No employee of the City shall have any personal or beneficial interest in the Services or property described in this Agreement. The Contractor shall not hire, or contract for services with, any employee or officer of the City that would be in violation of the City's Code of Ethics, D.R.M.C. § 2-51, *et seq*. or the Charter §§ 1.2.8, 1.2.9, and 1.2.12. The Contractor shall not engage in any transaction, activity or conduct that would result in a conflict of interest under this Agreement. The Contractor represents that it has disclosed any and all current or potential conflicts of interest. A conflict of interest shall include transactions, activities or conduct that would affect the judgment, actions or work of the Contractor by placing the Contractor's own interests, or the interests of any party with whom the Contractor has a contractual arrangement, in conflict with those of the City. The City, in its sole discretion, will determine the existence of a conflict of interest and may terminate this Agreement in the event it determines a conflict exists, after it has given the Contractor written notice describing the conflict.
32. **NOTICES**: All notices required by the terms of this Agreement must be hand delivered, sent by overnight courier service, mailed by certified mail, return receipt requested, electronic mail with read receipt requested, or mailed via United States mail, postage prepaid, if to the Contractor at the

aforementioned address, and if to the City at: Chief Information Officer, Denver Technology Services, 201 West Colfax Avenue, Dept. 301, Denver, Colorado 80202; with a copy to: Denver City Attorney's Office, 1437 Bannock St., Room 353, Denver, Colorado 80202. Unless otherwise provided in this Agreement, notices shall be effective upon delivery of the written notice. Notices sent by certified mail are effective upon receipt. Notices sent by mail are effective upon deposit with the U.S. Postal Service. If a Party delivers a notice through email and the email is undeliverable, then, unless the Party has been provided with an alternate email contact, the Party delivering the notice shall deliver the notice by certified or registered mail to the addresses set forth herein. The Parties may designate electronic and substitute addresses where or persons to whom notices are to be mailed or delivered. However, these substitutions will not become effective until actual receipt of written notification.

33. **DISPUTES**: All disputes between the City and the Contractor arising out of or regarding this Agreement will be resolved by administrative hearing pursuant to the procedure established by D.R.M.C. § 56-106(b)-(f). For the purposes of that administrative procedure, the City official rendering a final determination shall be the CIO as defined in this Agreement. In the event of a dispute between the Parties, the Contractor will continue to perform its obligations under this Agreement during the resolution of the dispute until this Agreement is terminated in accordance with its terms.
34. **GOVERNING LAW; VENUE**: This Agreement will be construed and enforced in accordance with applicable federal law, the laws of the State of Colorado, and the Charter, Revised Municipal Code, ordinances, regulations and Executive Orders of the City and County of Denver, which are expressly incorporated into this Agreement. Unless otherwise specified, any reference to statutes, laws, regulations, charter or code provisions, ordinances, executive orders, or related memoranda, includes amendments or supplements to same. Venue for any legal action relating to this Agreement will be in the District Court of the State of Colorado, Second Judicial District (Denver District Court).
35. **NO DISCRIMINATION IN EMPLOYMENT**: In connection with the performance of work under this Agreement, the Contractor may not refuse to hire, discharge, promote, demote, or discriminate in matters of compensation against any person otherwise qualified, solely because of race, color, religion, national origin, ethnicity, citizenship, immigration status, gender, age, sexual orientation, gender identity, gender expression, marital status, source of income, military status, protective hairstyle, or disability. The Contractor shall insert the foregoing provision in all subcontracts.
36. **LEGAL AUTHORITY**: The Contractor represents and warrants that it possesses the legal authority, pursuant to any proper, appropriate, and official motion, resolution or action passed or taken, to enter into this Agreement. Each person signing and executing this Agreement on behalf of the Contractor represents and warrants that he has been fully authorized by the Contractor to execute this Agreement on behalf of the Contractor and to validly and legally bind the Contractor to all the terms, performances and provisions of this Agreement. The City shall have the right, in its sole discretion, to either temporarily suspend or permanently terminate this Agreement if there is a dispute as to the legal authority of either the Contractor or the person signing this Agreement to enter into this Agreement.
37. **LITIGATION REPORTING**: If the Contractor is served with a pleading or other document in connection with an action before a court or other administrative decision making body, and such pleading or document relates to this Agreement or may affect the Contractor's ability to perform its

obligations under this Agreement, the Contractor shall, within 10 days after being served, notify the City of such action and deliver copies of such pleading or document, unless protected by law, to the City.

38. **LICENSES, PERMITS, AND OTHER AUTHORIZATIONS:** The Contractor shall secure, prior to the Term, and shall maintain, at its sole expense, all licenses, certifications, rights, permits, and other authorizations required to perform its obligations under this Agreement. This Section is a material part of this Agreement.
39. **NO CONSTRUCTION AGAINST DRAFTING PARTY**: The Parties and their respective counsel have had the opportunity to review this Agreement, and this Agreement will not be construed against any party merely because any provisions of this Agreement were prepared by a particular party.
40. **ORDER OF PRECEDENCE**: In the event of any conflicts between the provisions in the body of this Agreement, the Exhibits, or any other attachment hereto, the provisions in the body of this Agreement shall control. For the avoidance of doubt, no terms within any subsequent order form, invoice, or quote issued by the Contractor to the City shall be binding on the City or take precedence over the terms of the body of this Agreement regardless of any term contained therein to the contrary.
41. **SURVIVAL OF CERTAIN PROVISIONS**: The terms of this Agreement and any Exhibits and attachments that by reasonable implication contemplate continued performance, rights, or compliance beyond expiration or termination of this Agreement survive this Agreement and will continue to be enforceable. Without limiting the generality of this provision, the Contractor's obligations to provide insurance and to indemnify the City will survive for a period equal to any and all relevant statutes of limitation, plus the time necessary to fully resolve any claims, matters, or actions begun within that period. Furthermore, a grant of property or intellectual property rights to the City that by its terms continues for longer than the duration of this Agreement will survive expiration or termination of this Agreement, except termination for the City's breach of its obligations to pay for such property or rights. Promptly after termination or expiration of this Agreement, in whole or in part, the Contractor shall promptly return to the City all City Data and all other information provided by the City in such format as the City may reasonably require and permanently erase all copies thereof.
42. **INUREMENT**: The rights and obligations of the Parties herein set forth shall inure to the benefit of and be binding upon the Parties hereto and their respective successors and assigns permitted under this Agreement.
43. **TIME IS OF THE ESSENCE**: The Parties agree that in the performance of the terms, conditions, and requirements of this Agreement, time is of the essence.
44. **FORCE MAJEURE**: Neither Party shall be responsible for failure to fulfill its obligations hereunder or liable for damages resulting from delay in performance as a result of war, fire, strike, riot or insurrection, natural disaster, unreasonable delay of carriers, governmental order or regulation, complete or partial shutdown of manufactures, unreasonable unavailability of equipment or software from suppliers, default of a Subcontractor or vendor (if such default arises out of causes beyond their reasonable control), the actions or omissions of the other Party and/or other substantially similar occurrences beyond the Party's reasonable control ("Excusable Delay"). In the event of any such Excusable Delay, time for performance shall be extended for as may be reasonably necessary to compensate for such delay.

45. **PARAGRAPH HEADINGS**: The captions and headings set forth herein are for convenience of reference only and shall not be construed to define or limit the terms and provisions hereof.
46. **CITY EXECUTION OF AGREEMENT**: This Agreement is expressly subject to and shall not be or become effective or binding on the City until it has been fully executed by all signatories of the City and County of Denver.
47. **ADVERTISING AND PUBLIC DISCLOSURE**: The Contractor shall not include any reference to this Agreement or to Services performed pursuant to this Agreement in any of the Contractor's advertising or public relations materials without first obtaining the City' written approval. Any oral presentation or written materials related to Services performed under this Agreement will be limited to Services that have been accepted by the City. The Contractor shall notify the City in advance of the date and time of any presentation. Nothing in this provision precludes the transmittal of any information to City officials.
48. **EXTERNAL TERMS AND CONDITIONS DISCLAIMER**: Notwithstanding anything to the contrary herein, the City shall not be subject to any provision including any terms, conditions, or agreements, and links thereto, appearing on the Contractor's or a Subcontractor's website, forms, or any provision incorporated into any click-through or online agreements related to the Work unless that provision is specifically incorporated into this Agreement.
49. **PROHIBITED TERMS**: Any term included in this Agreement that requires the City to indemnify or hold the Contractor harmless; requires the City to agree to binding arbitration; limits the Contractor's liability for damages resulting from death, bodily injury, or damage to tangible property; requires payment for any obligation where there has not been an appropriation; requires venue and jurisdiction outside of the Colorado; or seeks to modify the order of precedence, as stated in the main body of this Agreement; or that conflicts with this provision in any way shall be *void ab initio*. All contracts entered into by the City, except for certain intergovernmental agreements, shall be governed by Colorado law notwithstanding any term or condition to the contrary.
50. **USE, POSSESSION OR SALE OF ALCOHOL OR DRUGS**: To the extent applicable, the Contractor shall cooperate and comply with the provisions of Executive Order 94 and Attachment A thereto concerning the use, possession or sale of alcohol or drugs. Violation of these provisions or refusal to cooperate with implementation of the policy can result in the City barring the Contractor from City facilities or participating in City operations.
51. **COUNTERPARTS OF THIS AGREEMENT**: This Agreement may be executed in counterparts, each of which shall be deemed to be an original of this Agreement.
52. **ELECTRONIC SIGNATURES AND ELECTRONIC RECORDS**: The Contractor consents to the use of electronic signatures by the City. This Agreement, and any other documents requiring a signature hereunder, may be signed electronically by the City in the manner specified by the City. The Parties agree not to deny the legal effect or enforceability of this Agreement solely because it is in electronic form or because an electronic record was used in its formation. The Parties agree not to object to the admissibility of this Agreement in the form of an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the ground

that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

53. **ATTACHED EXHIBITS INCORPORATED**: The following attached exhibits are hereby incorporated into and made a material part of this Agreement: **Exhibit A**, Scope of Work; **Exhibit B**, Requirements Traceability Matrix; **Exhibit C**, Integration Requirements Matrix; **Exhibit D**, Certificate of Insurance; **Exhibit E**, Information Technology Provisions; **Exhibit F**, HIPAA/HITECH BAA; and **Exhibit G**, Criminal Justice Information Services Security Addendum.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

Contract Control Number: TECHS-202473962-00
Contractor Name: NAPHCARE, INC

IN WITNESS WHEREOF, the parties have set their hands and affixed their seals at Denver, Colorado as of:

SEAL

CITY AND COUNTY OF DENVER:

ATTEST:

By: _____

_____

APPROVED AS TO FORM:

Attorney for the City and County of Denver

By: _____

REGISTERED AND COUNTERSIGNED:

By: _____

By: _____

Contract Control Number: TECHS-202473962-00
Contractor Name: NAPHCARE, INC

By: Signed by: Byron Harrison 3CBEB5D17BB74FB...

Name: Byron Harrison
(please print)

Title: Chief Information Officer
(please print)

ATTEST: [if required]

By: _____

Name: _____
(please print)

Title: _____
(please print)

Exhibit A – Statement of Work (SOW) and Implementation Services

1. NaphCare Obligations. Subject to terms and conditions of the Agreement and provided Customer is not in material breach of its obligations hereunder, NaphCare shall provide the following Implementation and Training Services during the Term:

1.1. Project. In order to provide an Electronic Health Record to Customer (the "Project"), NaphCare will implement the System which operates as a fully contained Electronic Health Record designed for the corrections industry. NaphCare shall plan, customize, configure, integrate, test, document, migrate, and deploy, the System and provide to Customer all deliverables in accordance with the requirements of this SOW and the Deliverables Chart set forth in Section II. Without limiting the generality of the foregoing, NaphCare shall provide all its personnel, equipment, accessories, tools and other items and do all work required for the Project where the same are not expressly identified in this SOW as being provided by Customer.

1.2. Project Change Request Process: If the Vendor scope outlined in this SOW must be altered (i.e., scope, schedule, or budget) regardless of if this alteration impacts the costs associated with the project, the following Change Request process will be adhered to:

1.2.1. Vendor will provide CCD with a Vendor Change Request, that details what the change is and at minimum the impacts to the scope, schedule, and budget. If warranted the Change Request should also include the risks, issues, and dependencies associated with the change.
1.2.2. The CCD Project Team will review the Vendor Change Request to ensure the full impact of the change is understood. If required CCD and Vendor will meet to ensure CCD completely understands the change being requested.
1.2.3. Upon the outset of the Change Request being identified, the CCD Project Manager will advise the CCD Project Sponsors of the Change and rough order of magnitude (i.e., small, medium, large) the anticipated impact it will have on the project.
1.2.4. Once the CCD Project Team has confirmed the impact of the change is completely understood, the CCD Project Manager will present the Change Request to the CCD Sponsors for formal approval.
1.2.5. Once a decision is rendered by the CCD Project Sponsors, the CCD Project Manager will provide the Vendor Project Manager with written/electronic notice of the decision and if approved the change will be officially added to the project scope. If the change is not approved, it will be dispositioned as an issue, risk, or closed by the CCD PM.
1.2.6. If the Change Request impact on the schedule risks or causes a work stoppage prior to the Change Request process being completed, the Vendor Project Manager and CCD Project Manager must work to expedite this process to avoid or at minimum reduce any work stoppage(s).

1.3. Implementation

1.3.1. Project Kickoff. NaphCare will hold a multi-day, on site meeting with all key parties involved in the Project. The event will include a full demonstration of the System in its foundational state for Customer stakeholders in addition to NaphCare staff having the ability to visit and observe representative prison facilities where the System will be deployed.

1.3.2. Project Plan. Within thirty (30) days following the execution of the Agreement, NaphCare will provide for Customer a phased, milestone-based, detailed **Project Plan, which will identify 3rd party vendor schedule, as applicable**. The Plan will be comprehensive, providing detailed timelines and milestones for the Services outlined herein and will be utilized to provide the Services defined herein.

1.3.3. Project Management Documentation. NaphCare shall collaborate with the Customer to document the various project management documents that may be included in, or supplementary to, the Project Plan:

i. Communication Plan
ii. Change Management Plan
iii. Risk Management Plan
iv. Resource Management Plan
v. Configuration Management Plan
vi. Project Status Reports

1.3.4. NaphCare will regularly review these documents and update as appropriate throughout the project.

1.3.5. Software Requirements Gathering. NaphCare is responsible for the configuration and/or customization of existing functionality of the standard System in order to meet the needs of the Customer. NaphCare shall hold multiple, domain specific requirements gathering meetings with Customer stakeholders focused on each functional area of the System. A **Software Requirements Document** shall be jointly prepared by the parties and will include all required modifications to the System including, but not limited to, the following functions and workflows:

i. Receiving/Intake, Release/Discharge Processes
ii. Nursing Encounter Protocols/Forms/Workflows
iii. Provider Encounter Protocols/Forms/Workflows
iv. Behavioral Health Protocols/Forms/Workflows
v. Medication Management Workflows
vi. Specialty Care Workflows
vii. Offsite Workflows and Network Loading
viii. Custom Reporting & Dashboards

Following requirements gathering and prior to Final System Acceptance, all revisions to previous customizations and/or new customizations shall be treated as Feature Requests pursuant to the process set forth in Section I, Subsection 1.7.

1.3.6. Interface Requirements Gathering. NaphCare is responsible for the development of interfaces by which the System sends and receives data from outside computer systems in order to meet the needs of the Customer. An **Interface Requirements Document** shall be jointly prepared by the parties and will include all technical definitions of, and specifications for, all required interfaces, including, but not limited to, the following:

i. Jail Management System (ATIMS)
ii. Medical Records (Denver Health/EPIC)
iii. Pharmacy System (Omnicell or EPIC Pharmacy System)
iv. Identity Provider of CCD (Azure AD)
v. Colorado Immunization Information System (CIIS)

vi. Lab Vendor/Provider (Denver Health/EPIC)
vii. Digital Radiology (Denver Health/EPIC)
viii. Dental Radiology (Sidexis?)
ix. Health Information Exchange (Contexture/CORHIO)

1.3.7. Cloud Services Design. NaphCare is responsible for configuration and deployment of the Cloud Hosting Services as defined in Section III. NaphCare will deploy the cloud environment on the schedule defined in the Project Plan an in accordance with a **Cloud Services Design Document** that is jointly developed by Customer and NaphCare and includes all aspects of the configuration of the cloud environment.

1.3.8. Development and Delivery. NaphCare shall develop necessary configurations, customizations, integrations and cloud services to meet the requirements defined in the Software Requirements Document, Integration Requirements Document, and Cloud Services Design Document. Customer is responsible for application deployment/access within Customer facilities.

1.3.9. Testing and Quality Assurance. NaphCare is responsible for the initial testing and quality assurance of the System based on the Software Requirements Document, Integration Requirements Document, and Cloud Services Design Document. NaphCare shall develop and deliver to Procuring Agency by the dates set forth in the Project Plan a Testing Plan by which the Customer will, with NaphCare's assistance, accurately determine whether the System and each deliverable conforms to the applicable Documentation. NaphCare shall develop and deliver to Customer by the dates set forth in the Project Plan suggested Acceptance Tests by which the Customer will, with NaphCare's assistance, accurately determine whether the System and each deliverable conforms to the applicable Documentation. Each such Acceptance Test shall set forth in adequate detail the expected results thereof and will focus on changes and customizations to the base Application. In addition, the Customer at its option may define certain additional acceptance criteria that it wishes to have included in the System Acceptance Test. Customer will document any Malfunctions identified during Acceptance Testing using a Problem Report. NaphCare will promptly correct any material Malfunctions and notify Customer when re-testing may be conducted.

1.3.10. Data Migration. NaphCare is responsible for the data migration activities limited to the import of data from existing medical record documentation and clinical validation of key data elements for the Customer's active Patient population. NaphCare and Customer agree to form a Data Migration Plan that details the approach to migrate data including but not limited to the following:

i. Medications
ii. Allergies
iii. Treatments
iv. Diets
v. Problem Lists and Special Needs
vi. TB Reads
vii. Mental Health Conditions and Substance Abuse
viii. Health and Physical Data
ix. Chronic Care Conditions
x. Lab and Radiology Data

xi. Scheduled Sick Call and Offsite Appointments
xii. Scheduled Diagnostic Tests

1.3.11. Training. NaphCare is responsible for pre-Go-Live and Go-Live training/support for all Authorized Users in order to support the management of and ongoing productive use of the System within the Customer's environment. Both end-user and super-user training will be provided via the following methods and be fully defined within a **Training and Go-Live Plan** that is jointly created by NaphCare and the Customer.

i. Introductory Remote Training via Online Meetings
ii. Pre Go-Live Onsite Classroom Training
iii. Go-Live Onsite Training and Support
iv. Train the Trainer Strategies

1.3.12. Documentation. NaphCare is responsible for the provision and ongoing updating of end-user and technical Documentation of the System in the following forms:

i. User's Manual
ii. Video Library
iii. Data Dictionary
iv. Knowledge Base online repository.

1.3.13. Go-Live. NaphCare is responsible for supporting Go-Live activities for use of the System within the Customer's Production environment. Go-Live scheduling will be defined in the **Training and Go-Live Plan** jointly created by NaphCare and the Customer.

1.3.14. The commitment for the completion and go-live of the overall EHR project shall be determined by both parties. NaphCare shall not be liable for any project delay(s) unless such delay(s) is (are) due to NaphCare's fault. Customer shall provide written confirmation to NaphCare of go-live start date two (2) weeks in advance of agreed upon date. Should Customer change go-live date within two (2) weeks preceding start date, Customer shall be solely responsible for all non-refundable costs incurred by NaphCare related to go-live activities. Such activities include but are not limited to: hotel accommodations, transportation costs, and personnel back-fill costs related to those individuals involved in the go-live training and implementation activates provided by NaphCare. Go-live start date shall not occur within 7 days of a national holiday.

1.3.15. Readiness. At such time as all Deliverables required by the Project Plan for Go-Live are delivered to Customer, and NaphCare determines that the System and Services are completed, installed and operational, then NaphCare shall provide Customer with written notice that the System is ready for Go-Live. Upon receipt of such notice, Customer will perform Pre-Live Acceptance in order to verify that (i) all required Deliverables have been delivered and accepted (ii) all reported material Malfunctions identified during Acceptance testing have been corrected or otherwise resolved and (iii) the System and Services are completed, installed and operational. Upon successful completion of Pre-Live Acceptance, Customer shall provide written confirmation to NaphCare of the Go-live start date two (2) weeks in advance of the

date. The Go-live start date shall not occur within seven (7) days of a national or Customer observed holiday.

1.3.15.1. Approach. NaphCare will plan to deploy system at all licensed sites simultaneously using a "Big Bang" approach. This approach will be further defined in the **Training and Go-Live Plan** jointly formed by NaphCare and the Customer.

1.3.15.2. Go-Live Support. NaphCare will provide Go-Live support during and following Go-Live for a period of up to one (1) week after the Go-Live date as a part of included Services. Such training/support will include 7 x 24 coverage as needed.

1.3.15.3. Final System Acceptance. Customer shall utilize system in a production capacity for a period of 90 days during which time Contractor agrees to address all deficiencies and enhancements. Deficiencies will be addressed without additional cost. Enhancement requests will be addressed up to 100 development hours being provided without additional cost as defined in Section I. Following the 90-day period, System is deemed accepted by Procuring Agency and the project moves into Maintenance and Support Services.

1.3.15.4. Minor Deviations. NaphCare may make Minor Deviations from defined Plan documents without obtaining prior written consent of Customer and shall give Customer prior written notification of any such planned deviation through the delivery of an updated status report (including a revised applicable Plan) which shows the impact, if any, of such deviations on the remainder of the Project.

1.3.15.5. Reporting and Status. NaphCare is responsible for providing Customer a detailed status report for each calendar month during the Project until Final System Acceptance as defined in Section II. The report will describe the progress of the Project, including, (i) an updated Project Plan reflecting any mutually agreed changes to the Project Plan or any changes resulting from Minor Deviations, (ii) a report updating the status of each Deliverable under development and Services being performed, (iii) a detailed description of the tasks and schedules as required to implement the System for the interim period until the next monthly status report, including the level of compliance with the Project Plan, (iv) a listing of the resources Customer is required to provide, in accordance with the Project Plan, during the subsequent calendar month, (v) a general updated description of the tasks and schedules required to implement the System for the remainder of the Project Plan, (vi) specific identification of all new tasks commenced by NaphCare, all ongoing tasks, and identifying any tasks which are overdue or behind schedule, and (vi) such other information as is customarily included in monthly status reports prepared by NaphCare, or which is reasonably requested by Customer.

2. Customer Obligations. Subject to terms and conditions of the Agreement and provided NaphCare is not in material breach of its obligations hereunder, Customer shall provide the following services during the Term:

2.1. Network Connectivity Services. Customer shall provide sufficient internal LAN Network Connectivity and WAN Connectivity for communication between Customer's Licensed Sites. Customer LAN and WAN networks will support at least 0.12Mbps per concurrent session with <40ms latency. Customer will support the efforts of NaphCare in providing Network Connectivity Services as defined in Section III.

2.2. Data Migration. NaphCare's ability to migrate Patient information is based on the availability of current sources of the information and NaphCare's ability to access that information. It is Customer's responsibility to ensure reasonable access to the information and support of the Data Migration efforts as appropriate. The following limitations exist with respect to data conversion efforts by NaphCare.

i. If not specifically outlined as a defined data element above and if not provided in a consumable format including appropriate patient identifiers, Contractor does not commit to its capabilities to import such data. Specifically, raw, or bulk databases or tables that require discovery, definition, and mapping or are otherwise unprepared in nature fall within this category. All efforts to import data within this characterization will be best effort and exceed scope of the data migration services outlined herein.
ii. Should encounter documents be provided in .pdf format, they will be imported in the same format as provided without the ability to "split" documents based on specific encounters or dates of service. A key delineating the relationship of a .pdf document to a patient identifier is required.
iii. Historical paper records import will use an on-demand paper chart scanning process based on the Procuring Agency's business rules. Contractor commits to making available a pre-production environment of the EHR which will allow Procuring Agency's staff to scan existing paper documentation into the EHR and relate it to a patient's chart. Paper record scanning and import performed by Contractor is not within the scope of this SOW.

2.3. Facilities and Access. Customer shall provide sufficient access and facilities and/or working space within a facility for NaphCare to complete its obligations pursuant to the terms of the Agreement.

2.4. Human Resources. Customer shall provide access to sufficient Subject Matter Experts (SMEs) whose knowledge of existing and future workflows will drive the customization of the Application to fit Customer's environment. Required SMEs include, but are not limited, to the following roles:

- Clinical Intake
- Behavioral Health Intake
- Schedule/Registration - Appointments (onsite)
- Nursing Supervisor
- Provider SME - Medical
- Provider SME - Behavioral Health
- Pill Call Nurse
- Pharmacy SME

- Laboratory SME
- Ancillary Services Lead (e.g., Dental assistant)
- Schedule/Registration - Appointments (offsite)
- Medical Records Supervisor
- Discharge Planner SME
- CQI SME
- Executive Administration
- Custody/Security SME

2.5. Documentation. The Customer shall provide supporting documentation related to workflows, clinical documentation forms, any other supporting information to aid the NaphCare's understanding of expected functionality of the System within the Customer's environment.

2.6. Security and Authentication. Customer shall assign a user ID and password to each Authorized User. Customer shall maintain or cause to be maintained the confidentiality of all such user IDs and passwords, including implementing and enforcing such policies and procedures as Customer deems appropriate thereto and Customer shall maintain adequate technical, physical, and procedural access controls and system security requirements and devices to ensure that access to the System by or through Customer is limited to duly authorized persons. Customer shall be solely responsible for all use or misuse of its user IDs and NaphCare shall have no obligation to monitor for or report any use or attempted use of Customer's user IDs. All such user IDs and passwords are deemed to be Confidential Information of Customer, and Customer shall take reasonable steps to ensure that its personnel not share user IDs or passwords and not attempt to access the System except as duly authorized. NaphCare shall not be liable to Customer for any loss or damage arising out of or relating to Customer's failure to maintain its obligations set forth in this section.

Section I – Maintenance and Support Services

1 NaphCare Obligations. Subject to terms and conditions of the Agreement and provided Customer is not in material breach of its obligations hereunder, NaphCare shall provide the following Services during the Term:

1.1 System Maintenance. NaphCare will maintain the System which operates as a fully contained Electronic Health Record designed for the corrections industry. NaphCare shall provide Application Updates to all modules of the System as a part this SOW. Without limiting the generality of the foregoing, NaphCare shall provide all labor, facilities, equipment, accessories, tools and other items and do all work required for the maintenance and support of the System where the same are not expressly identified in this SOW as being provided by Customer. Specifically, NaphCare shall:

1.1.1. Maintain the Application to provide the functionality defined in the Documentation.

1.1.2. Maintain compliance of the Application in all material respects with the warranties.

1.1.3. Provide all Application Updates along with updated user and operational Documentation. In consultation and coordination with Customer, install all Updates in the Test environment and, when Customer testing is completed, migrate all Updates to the Production environment.

1.1.4. Provide "first line support" for all incorporated Third Party Products. NaphCare will coordinate any required support and corrective action required from the third party vendors or suppliers that NaphCare cannot directly provide. NaphCare will apply all updates that the vendor of such Third Party Products provides to NaphCare. Finally, NaphCare will maintain compatibility and integration of the Application with the Third Party Products.

1.1.5. Maintain compatibility and integration with any third party outcome reporting tools, which have been implemented by Customer as part of the EHR Application. Should any of these packages be upgraded, Customer will notify NaphCare in advance, so that analysis and code changes can be implemented as quickly as possible.

1.1.6. Maintain comprehensive change control procedures to control software versions and releases. All changes to be implemented at Customer are at the discretion of the Customer Change Advisory Board (CAB).

1.1.7. Correct any Application Errors which are (i) reported by Customer or (ii) reported by other NaphCare clients, or (iii) identified by NaphCare, all within a reasonable period, depending upon the severity of the error. Application Error resolution is further described Subsection 1.2 below.

1.2 Application Error Resolution. During the Term, NaphCare will provide Application Error resolution services. Upon notification by Customer that a Severe Malfunction has occurred, NaphCare will, as soon as possible, diagnose the problem and determine if an Application Error is the cause. NaphCare will use continuous diligent effort to (i) correct the error or defect as soon as possible and provide an Application Update, or (ii) provide a reasonable workaround solution if the error or defect cannot be immediately corrected. NaphCare will provide periodic maintenance releases to distribute corrections to Application Errors (i) which have caused other Malfunctions, or (ii) which have been identified by other NaphCare customers or by NaphCare.

1.2.1 A Severe Malfunction refers to an instance where (i) the System is rendered unusable; (ii) the performance of the System is severely degraded; or (iii) Customer's use of the System for its intended purpose is materially impaired.

1.2.2 Cloud Hosting Services. NaphCare will provide Server Infrastructure services as defined in Section III.

1.2.3 Network Connectivity Services. NaphCare will provide the Network Connectivity services as defined in Section III.

1.2.3.1 Support.

1.2.3.2 Support Services. NaphCare will maintain a 24/7/365 Help Desk which includes live staffing by NaphCare employees with the required expertise to provide support for the System and associated deliverables as outlined herein. Help Desk services shall include, but not be limited to:

i. Assistance with Application function questions.
ii. Assistance in diagnosing and determining the cause(s) of and resolving System Malfunctions.
iii. Assistance with report generation questions.
iv. Assistance with general computer management, operating system software, or networking software questions related solely to the use of the Application.
v. Assistance in testing Application Updates supplied by NaphCare.
vi. Assistance using any non-production environments.

The term "assist" (or "assistance"), when used to describe Help Desk services, means a help that NaphCare will provide, including, without limitation, troubleshooting, providing advice, answering questions, providing diagnosis, and sharing information.

1.2.4 Service Level Agreement. NaphCare's Help Desk Services will be provided in accordance with the following Service Level Agreement (SLA).

In response to a Problem Report related to the System, NaphCare shall correct a reported Malfunction or provide a reasonable workaround sufficient to substantially mitigate the adverse effects of the problem on the normal use of the System. Customer agrees to reasonably assist NaphCare

in its efforts to diagnose the problem and correct a Malfunction by making available information, documentation, access to personnel, and testing reasonably requested by NaphCare from time to time to assist NaphCare in identifying and correcting the problem. From time to time at its discretion, NaphCare also may (i) implement new releases of the System that contain changes, updates, patches, and fixes, and (ii) deliver to Customer new releases of the client Application Software that contain changes, updates, patches, and fixes.

In the event a Malfunction exists due to an error in the Documentation, NaphCare may correct such Malfunction by providing corrected Documentation; provided, however, that no revision, modification, or update to Documentation shall eliminate or materially diminish any operational functionality of the Application previously described therein.

Customer's requests for support services shall be submitted by telephone (Critical Issues) or via NaphCare's online self service portal.

1.2.5 Service Level Agreement:

		IMPACT			
		All Deployments	Single Deployment	Business Unit	Individual User
Urgency	Critical	1	1	2	3
	High	1	1	3	3
	Medium	2	2	3	4
	Low	3	3	4	4

The above SLA and associated definitions below pertain only to those Services provided by NaphCare.

- Urgency
  - Critical - Mission critical service not available
    - System error/defect directly impacting patient care.
    - Application cannot be used.
    - No workaround, bypass or alternative is available.
  - High - Mission Critical module or portion of service not available
    - System error/defect directly impacting patient care.
    - A critical portion of the application cannot be used.
    - No workaround, bypass or alternative is available.
  - Medium - Unable to normally complete work, workaround is available
    - System error/defect negatively & substantially impacted operations, impact to patient care is manageable via workaround.
    - Application can be used.
    - Workaround, bypass or alternative is available.

- Low - Able to work, would assist with completion of work.
  - System error/defect is not critical. Impact is limited & no risk to patient care.
  - Application can be used.
  - Workaround, bypass or alternative is available.

- Impact
  - All Deployments – All deployments of the System across all customers are impacted.
  - Single Deployment – A single deployment of the System to a single customer, with one or more locations, is impacted.
  - Business Unit – A single business unit, or function, is impacted across one or many deployments.
  - Individual User – A single user is impacted.

Response & Resolution SLA

	Initial Acknowledgement	**Response**	**Resolution**
P1 Critical	5 Minutes	30 Minutes	24 Hours
P2 High	5 Minutes	90 Minutes	3 Days
P3 Medium	5 Minutes	5 Days	8 Days
P4 Low	5 Minutes	10 Days	20 Days

- **Initial Acknowledgement** – This is an automated response confirming we have received your issue. This is performed 24 hours a day, 7 days a week, 365 days a year.
- **Response** – This is the time it takes for an agent from the NaphCare Help Desk to respond to the issue reported.
- **Resolution** – The time it will take to work and resolve your reported issue.

1.2.6 Support Escalation Process

Tier	Responsibilities
Tier 0 - Super Users – DSD TMU Staff (Customer)	• At each Licensed Site, Customer will identify a "Super User" who will be trained to have a good overall working knowledge of the Hardware Devices and the System. The Super Users will assist local Authorized Users with general Hardware Device and Application problems. and will be able to generally distinguish between hardware, operating system, network and application errors If Tier 0 support is unable to resolve the problem, it will be referred to the Tier 1 Help Desk.

Tier 1 -
Help Desk (Customer)
	• Responsibilities include but are not limited to:
	  • Resolving service tickets involving system access problems, passwords, System downtime and Malfunctions not directly related to the Application
	  • Provide assistance in use of the Application and any related System component.
	  • Refer unresolved problems to NaphCare's Tier 2 Help Desk if related to NaphCare's System or Services.

Tier 2 – Help Desk (NaphCare)	• Functioning as an escalation point for unresolved Tier 1 problems. Responsibilities include but are not limited to: • Troubleshoot hardware and network problems related to NaphCare provided System or Services. • Troubleshoot all database integrity and performance problems. • Routine maintenance, deployment of Updates. • Resolve operational problems with Production deployment. • Coordinate problem resolution with all third party vendors (e.g., suppliers of Third Party Products, vendors supporting interfaces applications/systems). • Refer unresolved problems to NaphCare Tier 3 Help Desk.
Tier 3 – Help Desk (NaphCare)	• Functioning as a final escalation point for unresolved Tier 2 problems. Responsibilities include but are not limited to: • Provide "24 X 7" support to diagnose and resolve System Malfunctions. • Resolve problems with the EHR Application including all core functionality, interfaces and other middleware. • Resolve problems with any third party software which has been imbedded or integrated with the Application.

1.3 Conditions for Maintenance and Support Services. NaphCare's obligation to provide Maintenance and Support Services is conditioned upon (i) Customer's use of the Application in an information technology environment meeting the requirements set forth in the Documentation and (ii) Customer's having installed in accordance with NaphCare's instructions the latest (i.e., most current) version of the Application; provided, however, that NaphCare shall provide Maintenance and Support Services with respect to a prior version of an Application for at least three (3) months following delivery to Customer of an updated version of the Application. NaphCare shall extend support of a prior version of the Application beyond three (3) months if Customer, through its testing, is unable to accept the updated version of the Application.

1.4 Training. During the Term, NaphCare will provide ongoing, remote and on-site training for all Authorized Users in order to support the management of and ongoing use of the System within the Customer's environment. Training will be provided via the following methods and following a formal request by Customer.

vii. Remote Training via Online Meetings
viii. Classroom Training
ix. On the Job Training

1.5 Documentation. During the Term, NaphCare will update and maintain (i) an online User's Manual specific to the customizations made for Customer; (ii) a custom database Data Dictionary; and (iii) a Knowledge Base online repository. Online resources will be made available by an online Customer Portal.

1.6 Software Updates. NaphCare shall provide Updates to Customer as and when they become generally available, at no additional charge (including retrofit of all prior customizations and Feature Requests). NaphCare agrees to deploy any such Update, including any prior customizations and Feature Requests that are contained in the Production System, into the Test environment within ninety (90) days of release of the Update, unless otherwise directed by Customer. Upon successful testing of the new Update, Customer will provide notice of acceptance to NaphCare, and the parties will mutually agree on a scheduled date for the migration of the Update to the Production environment.

1.7 Post Go-Live Software Customization. Following Go-Live and Final System Acceptance, Customer may, in its discretion, request that NaphCare develop certain enhancements to the System desired by the Customer. NaphCare agrees to develop and install such Customer-requested enhancements, following the below process:

1.7.1 Feature Requests will be submitted to NaphCare by Customer via the System Online Portal along with detailed business and functionality requirements.

1.7.2 NaphCare will review and estimate the work effort required to implement the feature and notify the Customer accordingly.

1.7.3 Customer designee shall allow implementation (approve) or deny implementation of each Feature Request and will provide the priority of each approved Feature Request.

1.7.4 NaphCare shall commence work on all approved Feature Requests and shall provide updated information on a recurring basis including the Feature Request, its status, the hours worked to date and the estimated hours needed for completion of the Feature Request.

1.7.5 NaphCare shall include the Feature Request in a future version of the Application for Customer testing and acceptance.

1.7.6 Upon successful testing of the new Update (and completion of any required regression testing), Customer will provide notice of acceptance to NaphCare, and the parties will mutually agree on a scheduled date for the migration of the Update to the Production environment per I.1.1.

1.8 Hours Pool. NaphCare shall provide to Customer, as a part of the costs outlined in Section II, a total of one hundred (100) labor hours (hereinafter referred to as 'Hours Pool'). It is agreed that said Hours Pool shall be subject to the process as set forth above until such time that the Hours Pool is exhausted.

1.8.1 NaphCare shall maintain the accounting of the Hours Pool outlining the services rendered as identified in this SOW and shall provide a detailed report to Customer on a quarterly basis or other timeframe as agreed upon by both Parties.

1.8.2 Both parties agree that following the exhaustion of the Hours Pool, additional Post Go Live Software Customization will be performed at the rates defined in Section II. Customer shall also have the option of renewing the Hours Pool; in this event, an amendment will be executed by both parties memorializing this renewal.

2 Customer Obligations. Subject to terms and conditions of the Agreement and provided NaphCare is not in material breach of its obligations hereunder, Customer shall provide the following services during the Term:

2.1. Network Connectivity Services. Customer shall provide sufficient internal LAN Network Connectivity and WAN Connectivity for communication between Customer's Licensed Sites. Customer LAN and WAN networks will support at least 0.12Mbps per concurrent session with <40ms latency. Customer will support the efforts of NaphCare in providing Network Connectivity Services as defined in Section III.

2.2. Remote Access. Customer shall provide NaphCare remote access to Customer owned and maintained infrastructure supporting the application as necessary for NaphCare personnel to provide the Maintenance and Support Services set forth in this SOW. Failure of the Customer to provide access methods or properly maintain those methods outlined above will result in NaphCare being unable to provide certain Maintenance and Support Services as outlined in this SOW.

2.3. Facilities and Access. Customer shall provide sufficient access and facilities and/or working space within a facility for NaphCare to complete its obligations pursuant to the terms of the Agreement.

2.4. Human Resources. Customer shall provide reasonable access to sufficient Subject Matter Experts (SMEs) whose knowledge will assist with NaphCare providing the Services described herein. Examples of such SMEs include, but are not limited to, health care clinical and technical roles directly related to the use of the System in Customer's environment.

2.5. Security and Authentication. Customer's ongoing responsibilities are set forth in Section I, Subsection 2.

2.6. Supporting Hardware, Software and Services. Customer is responsible for providing and supporting software that may complement the System, but not be a part of it. Such supporting software includes, but is not limited to, the following:

- Office Productivity Software
- Dictation Software
- Clinical Reference Software
- Identity Management Services
- 2-Factor Authentication Services

- Operating System Patching
- Security of Network, Infrastructure
- Interface Vendor Services from 3rd Parties
- Computer Workstations (Desktop, Laptops, Tablets)
- Peripheral Printing Devices
- Peripheral Signature Capture Devices

Section II – Deliverables, Acceptance, Schedule and Fees[1]

1. Implementation Fee Schedule.

Phase	Deliverables	Cost
1. Planning and Project Start	Project Kickoff Meeting Onsite Boot Camp Provision of Hosted Test Environment Customer Acceptance of Project Plan	**$52,500.00**
2. Requirements and Design	Customer Acceptance of • Software Requirements Document • Interface Requirements Document • Hosting Design Document • Data Migration Plan	**$70,000.00**
3. Development, Delivery and Testing	Delivery of Tailored EHR System Delivery of Interfaces Completion of Customer Acceptance Testing Delivery of Hosted Production Environment Customer Acceptance of Training and Go-Live Plan	**$87,500.00**
4. Data Migration	Import and Clinical Review of Data UAT of Migrated Data Completion of Data Migration	**$43,750.00**
5. Training and End User Technical Documentation	Custom User's Manual, Data Dictionary Completion of Pre-Live Training Plan Knowledge Base online repository Pre-Live Acceptance	**$43,750.00**
6. Go-Live	System Transition/Activation Integration Transition/Activation Pre and Go-Live Training and Post-Live Support	**$35,000.00**
7. Acceptance and Close-Out	Final System Acceptance (90 days after Go Live)	**$17,500.00**
	Total Implementation Cost:	**$350,000.00**

1.1. Schedule. As consideration for performance of the Implementation and Training Services described herein, NaphCare shall invoice and Customer shall pay Implementation Fees based on the completion and acceptance of Deliverables as defined in Section II, Subsection 1. Each invoice shall be submitted based on the provisions of II.4.

2. License, Maintenance and Support Fee Schedule.

[1] The parties hereby agree and understand that Implementation Fees are separate and in addition to any Software licensing fees and/or other additional fees referenced herein.

2.1. Software and Cloud License Fees:

Phase (Date of service/invoice)	Deliverable	Cost
Year 1 (Contract Signing)	Software License	**$70,000.00**
	Support / Maintenance	**n/a**
	Hardware / Cloud Stand-up	**$12,500.00**
Year 2 (1 year post Contract Signing)	Software License	**$70,000.00**
	Support / Maintenance	**$200,000.00**
	Hardware / Hosting	**$25,000.00**
Year 3 (2 years post Contract Signing)	Software License	**$70,000.00**
	Support / Maintenance	**$210,000.00**
	Hardware / Hosting	**$25,000.00**
Year 4 (3 years post Contract Signing)	Software License	**$70,000.00**
	Support / Maintenance	**$220,500.00**
	Hardware /Hosting	**$25,000.00**
Year 5 (4 years post Contract Signing)	Software License	**$70,000.00**
	Support / Maintenance	**$231,525.00**
	Hardware / Hosting	**$25,000.00**
	Total Operational Costs:	**$1,324,525.00**

2.1.1. Schedule. As consideration for the Licenses and the performance of the Services described herein, NaphCare shall invoice and Customer shall pay the above fees annually, in advance, payable on the first day of the new contract year.

2.2. Additional Services:

Component	Inclusions	Annual Cost
SureScripts	• Medication History for Reconciliation	$0 Included
Direct Secure Messaging (DSM)	• Encrypted communication protocol to facilitate the secure exchange of electronic health information among healthcare professionals and organizations	$0 Included
Development Hours	• 100 Development Hours (use within 90 days post Go Live) (see Section I 1.7)	**$0 (included)**
Development Hours	• Feature development or customization Post Go Live/Post Warranty Period	**$220/Hour in Arrears $200/Hour in advance**
EPCS	• Electronic Prescription of Controlled Substances	**$1,700.00 Per provider**

2.2.1. Schedule. As consideration for provision of the Services described above, NaphCare shall invoice and Customer shall pay fees annually, in advance based on the Go-Live date.

3. Acceptance & Deficiency Procedure.

3.1. In the course providing of the Implementation and Training Services, NaphCare shall notify Customer when Deliverables defined in Section II, Subsection 1 are available for Customer review. Upon notification, Customer shall perform a review as Customer deems necessary to verify that the Deliverable conforms to the applicable specifications and/or functional criteria. If the Application or other component of the System is the Deliverable, Customer shall perform System testing to verify that the Deliverable complies with the Documentation and applicable warranties. If System Acceptance is the Deliverable, Customer will verify, through use of the System in a Production ("live") environment, that the System conforms to the warranties, the Documentation, and any other criteria set forth in the SOW and Implementation Plan. Unless Customer rejects the Deliverable by providing written notification to NaphCare via a Problem Report within thirty (30) days, Customer will be deemed to have accepted the Deliverable. Customer shall not unreasonably withhold acceptance of a Deliverable.

3.2. In the event that Customer rejects the Deliverable as provided herein, Customer shall notify NaphCare via the Problem Report. NaphCare shall then deliver to Customer promptly, but no later than thirty (30) days following notification via the Problem Report, a correction of the Deliverable with notice of Deliverable completion for Customer review.

3.3. In the event NaphCare is notified of a rejection of the Deliverable as described in the preceding clause, Customer shall make available all information reasonably requested by NaphCare to assist NaphCare in identifying the issue. For Application Errors that are not replicable on NaphCare's equipment, the parties shall attempt to verify that the Application Error exists on Customer's System. NaphCare shall retain the duty to correct Application Errors that are verifiable but not replicable on NaphCare's equipment.

3.4. The procedure described herein shall be repeated with respect to revised versions of the Deliverable that NaphCare provides to Customer until (i) Customer notifies NaphCare of its acceptance of the Deliverable (or is deemed to have accepted the Deliverable pursuant to Section 3.1), (ii) Customer makes a final rejection of the revised Deliverable after rejecting the same on at least two (2) prior occasions, or (iii) NaphCare notifies Customer of its determination that correcting the issue within the Problem Report is not technically possible or is outside the scope of the defined responsibilities of NaphCare outlined in this Exhibit, Subsection 1 and Section I, Subsection 1.

3.5. In the event Customer issues a final written rejection of the Deliverable pursuant to Subsection 3.4. above or NaphCare delivers to Customer the notice described in Subsection 3.4. above, then at Customer's option, within thirty (30) days thereafter, Customer may terminate this SOW Agreement as set forth under the Agreement.

4. Invoices. Invoice payment terms are set forth in the Agreement. Each invoice shall contain a minimum of the following information: invoice number and date; remittance address; bill-to and ship-to addresses of ordering department/division; Agreement number (insert

contract ID#); Customer's Purchase Order number; quantities; item or deliverable descriptions, unit prices, extensions; sales/use tax if applicable; and an invoice total.

5. Additional Implementation.

5.1. This SOW covers the Licensed Sites specified herein as Denver County Jail (DCJ) and Denver Detention Center (DDC). Should Customer request that additional Licensed Sites be added to this SOW for access to and use of the System and Services, the parties will amend this Contract and NaphCare will incorporate new Licensed Sites at the then current rates for implementation and maintenance and support of the System and Services.

5.2. Schedule. The invoices shall be submitted on the first day of the first calendar quarter following Customer's Acceptance of the applicable Go-Live of the additional facility and quarterly thereafter for the remainder of the Term. Each invoice shall reflect 25% of the annual fee.

5.3. For clarification and avoidance of doubt, other than the number of Licensed Sites, there are no other volume-based metrics (e.g., named users, concurrent users) which govern the fees for License, Implementation and Training Services, Maintenance and Support Services, or Hosting Services.

Section III – Cloud Hosting Services

1. NaphCare Responsibilities.

1.1. Server Infrastructure. NaphCare will provide a cloud hosted environment in order to remotely host the Application. All necessary network infrastructure, computer hardware, data storage, third party software (such as database software), technology, operating systems, and remote access software needed to remotely host the Application and the Customer Data will be provided by NaphCare. NaphCare will (i) monitor the infrastructure; (ii) provide backup and restoration services for the Application; (iii) coordinate preventative maintenance; and (iv) provide system management services including database maintenance (including database upgrade services), data archiving, system troubleshooting, production change control, and scheduled operational tasks. NaphCare shall be responsible for maintaining appropriate security measures, systems, and procedures designed to protect against anticipated threats or hazards to the availability, security or integrity of the Customer Data.

1.2. Data Location. NaphCare shall provide its services to the State and its end users solely from Amazon Web Services (AWS) data centers within the Continental United States. All storage, processing and transmission of State data shall be restricted to information technology systems within the Continental United States. NaphCare shall not allow its personnel or sub-contractors to store Customer data on portable devices, including personal computers, except as specified and allowed by the contract, and then only on devices that are used and kept at its data centers within the Continental United States. NaphCare shall permit its personnel and NaphCare to access Customer data remotely only to provide technical support and as specified or required by the contract.

1.3. Server Environments.

1.3.1. NaphCare will provide a System development environment ("Dev") in order to support the implementation including (i) Dev Application environment, (ii) Dev database services and storage, (iii) Dev file storage, and (iv) Dev interface services within NaphCare's infrastructure environment.

1.3.2. NaphCare will provide a System test environment ("Test") in order to support the ongoing productive use, including (i) Test Application environment, (ii) Test database services and storage, (iii) Test file storage, (iv) Test interface services.

1.3.3. NaphCare will provide a System production environment ("Production") in order to support the Go-Live (activation) and ongoing productive use, including (i) Production Application environment, (ii) Production database services and storage, (iii) Production file storage, (iv) Production interface services. The Production environment shall comply with the Service Level Agreement set forth in Section I, Subsection 1.3.1.

1.4. Network Infrastructure. NaphCare will provide Network Connectivity Services to support the connectivity of Customer to hosted Server Infrastructure as follows:

1.4.1. Internet. NaphCare will provide sufficient Internet services for the Hosted environment.

1.4.2. Static VPN over Internet. Network communication between NaphCare's datacenters and Customer's network via VPN in which Internet is provided by NaphCare at the Hosted environment and Internet is provided at Customer's Licensed Sites by Customer.

1.5. Service Level Agreement.

1.5.1. Availability Requirement. NaphCare shall make the System Available ninety-nine (99.67%) percent of the time. Availability is measured on a 7 X 24 basis during any calendar-month period, excluding Excusable Outages. NaphCare cannot be held responsible for services, software, or equipment not provided hereunder. The Availability percentage during the month will be calculated as follows:

- (Total hours during the month) minus (Total hours related to Excusable Outages) equals Maximum Hours
- [(Maximum Hours) minus (Total hours of unplanned downtime)] divided by (Maximum Hours) equals Availability percentage

1.5.1.1: **"Excusable Outage**" means unavailability (i) during Scheduled Maintenance, or (ii) caused by or resulting from negligent or intentional acts or omissions of Customer, its Affiliates, an Authorized User, their respective employees, agents, contractors, or vendors, or any other party gaining access to the Application due to any such negligent act or omission, or (iii) arising from Customer's direction that NaphCare ceases making the Application Available for use other than in the event of a material breach of the Agreement by NaphCare, or (iv) caused by outages of Customer's LAN, or (v) caused by outages of Network Connectivity not provided by NaphCare, or (vi) caused by outages of individual end-user devices (e.g., workstations, printers, and peripheral devices)."

1.5.1.2 **"Scheduled Maintenance"** means System downtime associated with or caused by (i) maintenance (patches), upgrades, or replacement of infrastructure, hardware, software, or telecommunications services provided as part of the Hosting Services; or (ii) maintenance (patches) or Updates (bug fixes) to the Application. Scheduled Maintenance shall also include System downtime for which NaphCare has notified Customer at least twenty-four (24) hours in advance and Customer has consented to such downtime.

1.5.2. Response Time Requirement. In the event that Authorized Users at one or more Licensed Sites experience degraded System response time such that the affected Authorized Users are no longer able to effectively perform core

workflows using the System, then Customer shall have the right to declare the period of such degraded System response time as unscheduled System downtime for the purpose of calculating monthly System Availability. NaphCare cannot be held responsible for services, software, or equipment not provided hereunder.

1.5.3. Data Backups. NaphCare will backup Customer data with a one (1) hour Recovery Point Objective ("RPO") and a four (4) hour Recovery Time Objective ("RTO"). Retention of backups will include daily backups for one (1) week, weekly backups for one (1) month, monthly backups for eleven (11) months, and yearly backups for two (2) years.

1.5.4. Redundancy. NaphCare will maintain redundant datacenters in Birmingham, Alabama and Las Vegas, Nevada. System Application data will remain in synchronization between datacenters within the one (1) hour RPO. Should the primary datacenter become damaged, destroyed, or otherwise unavailable for any reason, the Application will fail-over to the backup datacenter for continued System access. Testing of the failover capability may occur at the Customer's request with no more than one test during a 365-day period.

1.5.5. Audit. NaphCare shall maintain complete and accurate records of all transactions and information necessary to calculate or measure the service levels described (the "Service Level Data"). All Service Level Data shall be maintained by NaphCare throughout the Term of the Agreement. Not more than once in any twelve (12) month period during the Term of this Agreement, Customer or its designated representatives shall be entitled to (i) audit and inspect the Service Level Data during business hours upon reasonable notice to NaphCare and (ii) make copies and summaries of such Service Level Data.

2. Customer Responsibilities.

2.1. Network Infrastructure. Customer will provide Network Connectivity Services to support the connectivity of Customer endpoints to hosted Server Infrastructure as follows:

2.1.1. Customer shall provide sufficient internal LAN network connectivity and WAN infrastructure for Customer's Licensed Sites. Customer LAN and WAN networks will support at least 0.12Mbps per concurrent session with <40ms latency.

2.1.2. Customer shall provide sufficient Internet connectivity to support Customer endpoints accessing the Hosted environment. Customer Internet services will support at least 0.12Mbps per concurrent session with <40ms latency.

2.1.3. Customer will provide and support any network equipment which resides within Customer facilities which is required for implementation of connectivity.

2.1.4. Customer shall provide access to the use of enterprise network management services including, but not limited to, Domain Name Services (DNS) and Shared/Network Printing Services in order for proper Application functionality.

2.1.5. Customer shall provide and support a Static VPN over Internet in order to provide offline mode functionality (if applicable).

- Customer shall allow communication across port 443 for all end-user devices. Note some device integrations may require additional port availability which will be defined in the Interface Requirements Documents.

Exhibit B Requirements Traceability Matrix

ID	Requirement Type	Requirement Name	Requirement Description	MoSCoW Value	Requirement Compliance	Product/Module	Vendor Response
1	**Functional**	**DSHS Health Services**	**DSHS Health Services is a division of the Sheriff's department that provides medical care to incarcerated patients. This is the intake process that occurs when a patient is booked into jail. They will need to complete a health care screening in order to determine their next level care.**				
1.1	Functional	New Patient Record	As a Denver Health Employee, I need the ability to enter new patient information into the new EHR solution so that each patient has a medical record.	Should Have	Out-of-the-Box	TechCare has a simple Add New Patient button to create new medical records for incoming patients, if not done so via the offender management system integration/interface.	TechCare's preference is to obtain patient demographic data from the offender management system as the 'system of record'. Thereby, if a patient exists in Custody's system of record, they by-default have a medical record created in TechCare. This alleviates the need for manual chart creation by Denver Health Employees.
1.2	Functional	Patient Unique Identifier	As a Denver Health Employee, I need the ability to enter a unique identifier for each patient which is the inmate CD number so that this avoids any duplicates or errors of any patients that may have similar names.	Must Have	Out-of-the-Box	The Add New Patient button allows for entry of unique patient identifiers. The offender management integration would forgo the need for manual entry.	TechCare's preference is to obtain patient demographic data from the offender management system as the 'system of record'. Thereby, if a patient exists in Custody's system of record, they by-default have a medical record created in TechCare, automatically created using the inmate CD number.
1.3	Functional	Patient Questionnaire	As a Denver Health Employee, I need the ability to complete a questionnaire in the new system so that we can determine if the patient needs immediate care.	Must Have	Out-of-the-Box	Booking Queue > Receiving Screening (form) or simply Receiving Screening button on patient chart main screen.	The out-of-the-box Receiving Screening captures vital medical information following a proactive care model aimed at identifying acute and chronic issues immediately at the patient's first screening. Examples of items captured: Vital Signs (with prompts for out-of-range values), Chronic Conditions, Substance Use questionnaires designed to prompt detox protocols/screenings, and a patient's Mental Health baseline.
1.4	Functional	Patient Returns from Outpatient Health Care Appointment	As a Denver Health Employee, I need the ability to enter a patien'ts medical appointment in the new EHR system so that we know where a patient is in the process.	Should Have	Out-of-the-Box	Appointment/Sick Call Viewer Booking Queue	TechCare's out-of-the-box solution contains a booking queue to confirm each patient receives proper screening (Receiving, Mental Health, TB, Informed Consents). Out-of-the-box, TechCare also contains built-in tools for managing clinic schedules across a multitude of appointment types (Dental, Chronic Care, Provider, Nurse RN, etc.).
1.5	Functional	Charting	As a Denver Health Employee, I need the ability to access other clinical information while charting so that I can make notes to a patients medical history.	Must Have	Out-of-the-Box	Multi-Window operation / controls to allow review from multiple areas of the chart.	Most modules/features of TechCare are accessible in multiple areas. For example, from an intake/receiving screening form, you can also review Vitals history that may have already been entered on the chart by another clinician. Likewise, the patient's chart can be opened in a separate browser window to access all other chart data, with the ability to return to the prior tab and finish the Receiving Screening (or any form/data entry point being completed).
1.6	Functional	Multi-Task Charting	As a Denver Health Employee, I need the ability to access multiple screens while charting so that I can create tasks, order labs, etc. while updating a patients chart.	Must Have	Out-of-the-Box	Multi-Window operation / controls to allow review from multiple areas of the chart.	Similar to comments in requirement 1.5, many built in forms/screenings contain shortcut buttons to enter drug, lab, radiology orders, appointments, separate progress notes in real-time vs. navigating away to a separate area of the chart.
1.7	Functional	Upload PDF, Fax	As a Denver Health Employee, I need the ability to interface, upload and attach documents/pictures/files to a patients profile so that the staff can review when needed. (PDF, MS Word, MS Excel, GIF, JPEG)	Must Have	Out-of-the-Box	Patient Main Screen > Attach Documents	The main screen of all patient charts (commonly referred to as "History Window" has a simple Attach Documents link/button and the capability to use drag and drop functionality if link/button is not user preference over drag and drop.
1.8	Functional	Uploaded Medical Documents	As a Denver Health Employee, I need the ability to review medical documents from outside provider(s) that have been uploaded into the system so that I can determine next level care.	Must Have	Out-of-the-Box	Provider's Queue > Records Review	Documents scanned in meeting certain criteria are automatically displayed within TechCare's Provider's Queue > Records Review tab for Provider Sign-Off.
1.9	Functional	Patient Returns from Inpatient Hospital Stay	As a Denver Health Employee, I need the ability to enter or update patient information and answer any questions in the system that pertain to the patient so that I can determine next level care.	Should Have	Out-of-the-Box	Forms, Progress / SOAP Notes, Monitoring Queues, Nursing Protocols	All items to the left in addition to simple data entry screens related to ordering, vitals, blood glucose entries and plenty other items are always available and accessible for charting. Additionally, TechCare allows concurrent charting so two users can be working on a chart at the same time with no locking of records.
1.10	Functional	Ongoing Health Care	As a Denver Health Employee, I need the ability to request care on behalf of patients so that they can continue with medical treatment.	Should Have	Out-of-the-Box	Sick Calls / Appointments	If this requirement is related to handling of patients' Health Needs Requests (kites or sick call requests), creating sick calls is very straight forward in TechCare. If the patients requests these via a paper process, they can be easily attached to their health record. Additionally, we have experience with automated entry of sick calls into TechCare from tablets and kiosks.
1.11	Functional	Patient Released	As a Denver Health Employee, I need the ability to change the status of a patient to release so that we know where the patient is in the process and that we can look into next steps to assist the patient.	Should Have	Out-of-the-Box	Patient Active / Not Active Status and Discharge Planning module.	TechCare's preference is to obtain patient demographic data from the offender management system as the 'system of record'. Thereby, is released or has an upcoming release, this information is automatically displayed. Additionally, there is an out-of-the-box Discharge Planning module to confirm all discharge needs are completed as required.
1.12	Functional	Patient Services	As a Denver Health Employee, I need the ability to enter notes for services provided to a patient so that we know what type of services are being provided to a patient once released.	Must Have	Out-of-the-Box	Discharge Planning module	The discharge planning module consolidates all release planning activities, which are displayed grouped together on the patient's chart for review in-real-time and post-release.
1.13	Functional	Order Sets	As a Denver Health Employee, I need the ability to provide order sets for patients based on a specific diagnosis so that a set of tests and/or panels and medications are performed based on the patients condition. (i.e. opioids, alcohol, etc.)	Must Have	Out-of-the-Box	Templates / Guidelines Detox Dashboard/Queue	The templates and guidelines module of TechCare allows for building of order sets. Additionally, out-of-the-box protocols are available for detoxing patients (CIWA, CIWA-B, COWS).
2	**Functional**	**DSHS Dental Workflow**	**DSHS Dental is the onsite dental exam office in which patients are seen for their routine dental exams.**				

ID	Requirement Type	Requirement Name	Requirement Description	MoSCoW Value	Requirement Compliance	Product/Module	Vendor Response
2.1	Functional	Dental Exam Request	As Denver Health Employee, I need the ability to submit a KITE/Patient Health Care Request on behalf of a patient so that they can receive a dental exam. (This could be a flag that is triggering an alert that a patient needs a dental exam. The vendor can suggest the best option.)	Should Have	Out-of-the-Box	Sick Calls / Appointments	Creating sick calls is very straight forward in TechCare, which essentially builds the Clinic list (whether dental, nursing, provider, psych-related). If the patients requests these via a paper process, they can be easily attached to their health record. Additionally, we have experience with automated entry of sick calls into TechCare from tablets and kiosks.
2.2	Functional	Dental Exam Schedule	As a Denver Health Employee, I need the ability to request the dental exam schedule so that we know what patients need to be escorted to the dental exam room, what date and time.	Must Have	Out-of-the-Box	Appointment/Sick Call Viewer	The clinic list can be pulled and filtered as much as the user sees fit, then printed or exported easily to provide for custody export. This even includes out-of-the-box a "Print for Officer" option that removes the reason for exam and HIPAA related information.
2.3	Functional	Dental Charts	As a Denver Health Employee, I need the ability to pull a patients dental history and review patient dental charts so that they can be reviewed prior to a dental exam and so the medical staff knows what medications the patient is using or has used in the past.	Should Have	Out-of-the-Box	History Window	TechCare's History Window is easily filter-able by record category or name (i.e. Dental only). This would display only the patient's dental-related information with a few clicks of a button for easy review before they come to clinic. The filter also remains on for the next patient chart that is opened, so the dental clinicians could move from chart to chart without having to rest their filter on each new chart opened during that session of use in TechCare.
2.4	Functional	Diagram of the Mouth	As a Denver Health Employee, I need the ability to pull up the diagram of the mouth so that I can document a patients dental history in relation to the diagram.	Should Have	Out-of-the-Box	Dental Forms / Odontogram technology	TechCare's out-of-the-box Dental form contains an interactive tooth chart for documentation and also has Odontogram technology for charting.
2.5	Functional	Dental KOP (Keep On Person) Sign Out	As a Denver Health Employee, I need the ability to sign out KOP (Keep On Person) medications so that there is a record of the medications that are needed for a patient.	Should Have	Out-of-the-Box	eMAR	The eMAR's built-in functionality has "Administered/Delivered KOP" designations to document KOP medications and quantity given.
2.6	Functional	X-Rays	As a Denver Health Employee, I need the ability to upload dental x-rays so that there is a record of the patients dental images.	Must Have	Out-of-the-Box	Patient Main Screen > Attach Documents	The main screen of all patient charts (commonly referred to as "History Window" has a simple Attach Documents link/button and the capability to use drag and drop functionality if link/button is not user preference over drag and drop.
2.7	Functional	Dental Patient Orders	As a Denver Health Employee, I need the ability to review and process medication orders so that patients receive their prescribed medications.	Should Have	Out-of-the-Box	Drug Orders / Emar	TechCare's origins are from a simple eMAR strictly for med administration documentation. TechCare's drug order entry screen also allows multiple orders to be entered at once shopping-cart-style for efficient medication ordering.
3	**Functional**	**DSHS Infectious Disease Caseworker Workflow**	**DSHS Infectious Disease is the division of the Denver Sheriff Health Services that provides medical care to those patients with HIV. This division may also deal with transgender patients.**				
3.1	Functional	Review Infectious Disease Logs	As a Denver Health Employee, I need the ability to review infectious disease logs, labs and MAR's so that I can schedule appointments for patients in order receive treatment and access medication.	Should Have	Out-of-the-Box	Reports, Advanced Search, patient History Window, Emar	This requirement is fulfilled out-of-the-box via many modules. An infectious disease log can be pulled through a simple report or Advanced Search for patients flagged with specific disease(s). Once opening a chart, the prior lab results are seen at the bottom-right of the patient's history window and can be opened to view results. Above those lab results, the patient's current medications are easily viewable and opened. Additionally, one click of a button takes you to the patient's MAR to view all historical, current and future medications.
3.2	Functional	Upload Disease Log, Labs and MAR's	As a Denver Health Employee, I need the ability to upload disease logs, labs and MAR's into the new EHR system so that we have a record of a patients medical history.	Should Have	Out-of-the-Box	Patient Main Screen > Attach Documents	Any chart-worthy item with a standard file type (not just limited to PDF documents) are able to be uploaded via TechCare's attach document features. We also have the capability to interface with lab partners to eliminate the manual need for uploading labs into charts. TechCare's medication ordering functionality and out-of-the-box MAR/eMAR eliminate the need for paper MARs and uploading.
3.3	Functional	HIV Referral Log	As a Denver Health Employee, I need the ability to review the HIV referral log so that I have a list of patients and am able to review their labs and MAR (Medication Administration Record) if available.	Should Have	Out-of-the-Box	Appointment/Sick Call Viewer	TechCare's built-in Sick Call/Appointment Viewer is the one-stop shop for viewing a referral log/clinic list. From there, individual charts can be opened to review labs and MAR.
3.4	Functional	Internal Referrals	As a Denver Health Caseworker, I need the ability to fill out an internal referral so that patients are scheduled to the social work line and case manager so they are set up with housing and financial assistance prior to being released.	Should Have	Out-of-the-Box	Discharge Planning module	The discharge planning module consolidates all release planning activities, which are displayed grouped together on the patient's chart for review in-real-time and post-release. This module can contain tasks for all disciplines (Nursing, Providers, Social Workers, etc.)
3.5	Functional	External Referrals	As a Denver Health Caseworker, I need the ability to fill out an external referral so that patients are set up with housing and financial assistance prior to being released.	Should Have	Out-of-the-Box	Forms / External Links	External referral forms can be added to TechCare forms (point, click, narrative style text boxes) or an external fillable PDF can be easily accessed via External Links. Once completed, the PDF can be saved to the patient chart and forwarded to external entities for housing and financial assistance.

ID	Requirement Type	Requirement Name	Requirement Description	MoSCoW Value	Requirement Compliance	Product/Module	Vendor Response
4	**Functional**	**DSHS Intake / Patient Initial Arrival**	**The DSHS Intake and Patient Arrival is the process is when a patient is checked in to when they are in need of medical care.**				
4.1	Functional	Patient Injury	As a Denver Health Employee, I need the ability to document injury information for a patient so that I can determine if a patient is medically cleared for prebook.	Should Have	Out-of-the-Box	Rapid Receiving Screening form / Comprehensive Receiving Screening form	TechCare's out-of-the-box Receiving Screening captures injury information as the first line of defense for understanding whether a patient is cleared for jail or a Rapid Receiving Screening option is available for quick assessment to determine if the patient should be cleared for booking.
4.2	Functional	Suicidal Process	As a Denver Health Employee, I need the ability to document if a patient is suicidal so that I can escort the patient to an exam room.	Should Have	Out-of-the-Box	Flags and Suicide Watch Admissions Management module	Suicidal patients are logged via the Admissions Management, Suicide Watch module. This allows for frequency/time-based documentation when suicidal patients are rounded upon. These timed checks are user-based and can be set at a threshold of as little as 1 minute (constant observation). Built in forms are also available to update this timing frequency based on how acute the patient's suicidal ideations are.
4.3	Functional	Health Services Questionnaire	As a Denver Health Employee, I need the ability to complete the health services questionnaire so that I can determine if medications or medication items are ordered or administered and documented.	Should Have	Out-of-the-Box	Receiving Screening / Concurrent Charting	TechCare has out of the box Receiving Screening documentation that captures health information for the patient upon entry into the facility, including whether or not they have any acute or Chronic illnesses and if they are currently taking medication. That medication information is captured and sent to drug reconciliation queue to be worked by staff for verification of medications outside of the facility and the medications can easily be ordered for the patient from that same queue. Additionally, TechCare can be integrated with Surescripts to automate the medication reconciliation process for those connected pharmacies.
4.3.1	Functional	Allergies	As a Denver Health Employee, I need the system to auto populate the allergies of a patient so that I can assess a patients known allergies and determine if treatment or medication is needed.	Should Have	Out-of-the-Box	History Window	A patient's allergies are displayed front and center from the main screen / history window on a patient chart. Additionally, med-to-med and med-to-allergy interaction checks occur at the point of entry on medications, so allergies are considered electronically during that time and not solely reliant upon human intervention if a clinician forgets to look at the allergies before ordering a medication.
4.3.2	Functional	Special Diet	As a Denver Health Employee, I need the system to communicate with the JMS system so that the kitchen staff is made aware of any special dietary restrictions that a patient may have.	Should Have	With Configuration	Diets / JMS Integration / Daily Report Sender	One of the first items we work on in implementations is a feed with the JMS system. This feed can be unidirectional (demographics from JMS create TechCare medical charts) or bidirectional (where we would send dietary restrictions along with other alert data). We also have the ability to auto daily reporting of diets to various custody or kitchen staff.
4.3.3	Functional	Medication	As a Denver Health Employee, I need the system to automatically generation the medication verification sheet so that I can determine what medications a patient is taking (include type used, amount, and time of last use).	Should Have	Out-of-the-Box	Receiving Screening / Med Reconciliation / SureScripts / MAR	TechCare has out of the box Receiving Screening documentation that captures health information for the patient upon entry into the facility, including whether or not they have any acute or Chronic illnesses and if they are currently taking medication. That medication information is captured and sent to drug reconciliation queue to be worked by staff for verification of medications outside of the facility and the medications can easily be ordered for the patient from that same queue. Additionally, TechCare can be integrated with Surescripts to automate the medication reconciliation process for those connected pharmacies.
4.3.4	Functional	Dental	As a Denver Health Employee, I need the new EHR system to automatically schedule a dental exam so that if a patient has severe dental pain upon incarceration, an exam can be scheduled for them to be seen.	Should Have	Out-of-the-Box	Receiving Screening	When a patient answers that they have acute dental needs or pain on the Receiving Screening, a dental exam/sick call is automatically scheduled. With Denver Health employee's feedback, we will configure this timing to be based on the Dental clinic's schedule (i.e. within one week of entry or within 1 day of entry, etc.).
4.3.5	Functional	Mobility Issues	As a Denver Health Employee, I need the new EHR system to communicate with the JMS system so that there is documentation if a patient has mobility issues, artificial devices (wheelchair, crutches, dentures, etc.), or special health requirements.	Should Have	With Configuration	JMS Integration	One of the first items we work on in implementations is a feed with the JMS system. This feed can be unidirectional (demographics from JMS create TechCare medical charts) or bidirectional (where we would send dietary restrictions along with other alert data).
4.3.6	Functional	Pregnancy	As a Denver Health Employee, I need the ability to document if a patient is pregnant so that the JMS system is notified and that the patient is automatically taken through the pregnancy protocol.	Should Have	With Configuration	JMS Integration	One of the first items we work on in implementations is a feed with the JMS system. This feed can be unidirectional (demographics from JMS create TechCare medical charts) or bidirectional (where we would send dietary restrictions along with other alert data, to include pregnancy).
4.3.7	Functional	Drugs/Alcohol	As a Denver Health Employee, I need the ability to document if a patient has drug or alcohol issues so that they are automatically taken to withdrawal protocols.	Should Have	Out-of-the-Box	Receiving Screening > Comprehensive Detox Screen > CIWA / Detox Dashboard.	Out of the box, TechCare's Receiving Screening captures alcohol-use information and, using an algorithm based on last use will prompt for a Comprehensive Detox Screen. From the Comprehensive Detox Screen, the CIWA is also automatically prompted based on how the patient responds and automatically enrolls the patient into withdrawal monitoring and protocols.
4.3.8	Functional	Suicidal/Violent Thoughts/Self Harm	As a Denver Health Employee, I need the ability to document if a patient is suicidal, having violent thoughts or self harming so that I can automatically take them through a suicide screening.	Should Have	Out-of-the-Box	Columbia Suicide Screening Form, Flags and Suicide Watch Admissions Management module	Out of the box, TechCare has the Columbia Suicide Screening form to document a patient's level of suicidal ideation. This form uses programming to also place the patient on Suicide observation in the Admissions Management, Suicide Watch module. This allows for frequency/time-based documentation when suicidal patients are rounded upon. These timed checks are user-based and can be set at a threshold of as little as 1 minute (constant observation). Built in forms are also available to update this timing frequency based on how acute the patient's suicidal ideations are.
4.3.9	Functional	Mental Health History	As a Denver Health Employee, I need the ability to document if a patient has any mental health history so that I can automatically schedule a mental health assessment.	Should Have	Out-of-the-Box	Receiving Screening / Mental Health Screening	Out-of-the-box, TechCare's Receiving and Mental Health Screening forms have questions related to previous mental health history.

ID	Requirement Type	Requirement Name	Requirement Description	MoSCoW Value	Requirement Compliance	Product/Module	Vendor Response
4.3.10	Functional	Neurological	As a Denver Health Employee, I need the ability to document if a patient has any neurological disorders so that a neurological sheet is automatically generated and the patient is assessed.	Should Have	Out-of-the-Box	Receiving Screening	Upon entering the facility, the Receiving Screening form that is completed contains areas to document acute and chronic conditions to include neuro disorders. With configuration, this form can be configured to automatically order neuro checks or follow-up automatically based on answers supplied on the form.
4.3.11	Functional	Hospital Return	As a Denver Health Employee, I need the ability to screen a patient and document vital signs (temperature, blood pressure, pulse, respiratory, and oxygen) in the system within 30 minutes of a hospital return so that we have a record of their vital signs upon their return.	Should Have	Out-of-the-Box	ER / Off-Site / Hospital Return Form	TechCare's ER/Off-Site/Hospital Return form serves as a data entry point for staff to document vitals and other pertinent information when a patient returns to the facility. Additionally, any documentation from the outside entities that is scanned it, automatically flows to the Provider's Queue for review and sign-off.
4.3.12	Functional	Sexual Assault	As a Denver Health Employee, I need the ability to document if the patient is a victim of sexual assault so that a referral to psychology for evaluation is automatically generated.	Should Have	Out-of-the-Box	Receiving Screening	Upon entering the facility, the Receiving Screening form that is completed contains areas to document sexual assault and PREA-related questions (whether victim or perpetrator). With configuration, this form can be configured to automatically order any necessary evaluations or clinic visits with psych and/or PREA coordinators.
4.3.13	Functional	Potentially Infectious	As a Denver Health Employee, I need the ability to document if the patient is potentially infectious so that an alert is sent to JMS identifying that the patient needs to be isolated as a precaution.	Should Have	With Configuration	JMS Integration	One of the first items we work on in implementations is a feed with the JMS system. This feed can be unidirectional (demographics from JMS create TechCare medical charts) or bidirectional (where we would send dietary restrictions along with other alert data, to include pregnancy and infectious disease information). This data can be used for classification and housing decisions made by custody.
4.3.14	Functional	Bottom Bunk/Tier Restriction/Housed with Other Patients	As a Denver Health Employee, I need the ability to document restrictions for each patient (bottom bunk, tier restriction, and housed with other patients) so that an alert can be sent to JMS identifying that the patient needs to be accommodated due to these restrictions.	Should Have	With Configuration	JMS Integration	One of the first items we work on in implementations is a feed with the JMS system. This feed can be unidirectional (demographics from JMS create TechCare medical charts) or bidirectional (where we would send dietary restrictions along with other alert data, to include pregnancy, infectious disease information, mobility needs related to tier and bunk needs, etc.). This data can be used for classification and housing decisions made by custody.
4.4	Functional	Prebook	As a Denver Health Employee, I need the ability to complete the Recommendations for Classification form so that I can give this form to prebook and the patient is returned to seating or their cell.	Should Have	With Configuration	TechCare Form Builder	Virtually any form on paper today can be transformed into a form within TechCare. The Recommendations for Classification form can easily be added, along with automation and flow of it back to the JMS system via integration or the form can be emailed and sent to custody to help alleviate manual efforts for medical and custody staff.
5	**Functional**	**DSHS Optometry Workflow**	**The DSHS Optometrist determines if a patient has glasses and/or has received a prescription for glasses, they provide an eye exam and determines if the patient needs new glasses.**				
5.1	Functional	DSHS Scheduler	As a Denver Health Employee, I need the ability to pull up a list of eye exam patients so that I can determine if a patient is on the list or has received glasses within the past two years.	Should Have	Out-of-the-Box	Appointment / Sick Call Viewer	TechCare's appointment / sick call viewer is a one-stop-shop glance of the clinic's schedule, based on selection. In this scenario, the health employee could see who is on the upcoming schedule. From there, they can easily open the patient's chart and filter to their individual appointments > those related to eye exams and view whether the patient has glasses flagged on the chart and quickly find documentation associated with his/her last eye exam.
5.1.1	Functional	Eye Exam Waitlist	As a Denver Health Employee, I need the ability to place a patient on an eye exam wait list so that the patient can be scheduled for an eye exam with the optometrist who comes to the DDC & County Jail once a month.	Should Have	Out-of-the-Box	Appointment / Sick Call Viewer - OR - Onsites/Utilization Management	For contracted providers that come once per month, the UM module of TechCare can be used for this scheduling.
5.2	Functional	Prescriptions Scanned	As a Denver Health Employee, I need the ability to scan optometrist prescriptions into the clinic scheduler so that the patients prescriptions can be fulfilled.	Should Have	Out-of-the-Box	Attach Documents	The main screen of all patient charts (commonly referred to as "History Window" has a simple Attach Documents link/button and the capability to use drag and drop functionality if link/button is not user preference over drag and drop. Additionally, records like prescriptions for glasses can be attached directly into an individual sick call for association with that particular encounter.
5.3	Functional	Email Prescriptions	As a Denver Health Employee, I need the ability to email prescriptions within the system to an outside source so that the patients prescriptions can be fulfilled and that they are on file underneath the patients name.	Should Have	Out-of-the-Box	Direct Clinical Messaging	With configuration, TechCare is fully integrated HISP and can send clinical messages to other accepting entities, to include eye prescriptions. Medication orders are sent via pharmacy integration.
5.4	Functional	Eyeglass e-Signature Agreement	As a Denver Health Employee, I need the ability to e-sign eyeglass agreement with patients so that they can receive their prescriptions and that the form can be filed in the patients chart.	Should Have	Out-of-the-Box	Digital Signature / Patient Signature	All forms within TechCare completed by the clinicians while logged in are e-signed and contain logged data for the clinician. The forms also prompt for inmate signature, where necessary for patient signature.
6	**Functional**	**DSHS Medication Room – Patient Medication Administration Workflow**	**The DSHS Health Services Provider, verifies patient medications so that prescriptions can be filled and that appropriate medication is on hand.**				
6.1	Functional	Verify Medication	As a Denver Health Employee, I need the ability to view a list of all patient medications under a patient file so that they are can be transcribed on the patient MAR (Medical Administration Record).	Should Have	Out-of-the-Box	eMAR	There is no need for transcription of medication orders from a patient file onto their MAR in TechCare. TechCare's eMAR automatically displays all patients meds at an individual level and, likewise, serves as the mechanism to build med pass lists.

ID	Requirement Type	Requirement Name	Requirement Description	MoSCoW Value	Requirement Compliance	Product/Module	Vendor Response
6.2	Functional	Auto Renew Medication	As a Denver Health Employee, I need the ability to auto renew a prescription for a patient so that they are automatically auto dispensed 90 days of medication. I also need the ability to distinguish between medical and psychiatric drugs.	Should Have	Out-of-the-Box	Drug Order Entry / Drug Reorder/Refill Queues	TechCare's drug order entry has designated checkbox style data entry to delineate whether the medication is a medical or psychiatric medication. Likewise, there is a drug reorder/refill queue that is used to easily refill and reorder expiring medications or medications that are nearing the need for a refill.
6.3	Functional	Medication Information	As a Denver Health Employee, I need the ability to view medication information for a patient so that the patient understands the medicine that they are being prescribed and if there are any interactions that they need to be aware of.	Should Have	Out-of-the-Box	Drug Information module / drug-to-drug and drug-to-allergy interaction checks	TechCare is integrated and kept up-to-date on a monthly basis with MediSpan data. Using that data, a Drug Information module is easily accessible to pull the full description of the drug information as a free-world pharmacy would provide on information sheets. At the point of entry, TechCare performs drug-to-drug and drug-to-allergy interaction checks. When an interaction occurs, full details are provided and the user can either proceed to order (override the interaction) or choose an alternate medication.
6.4	Functional	Medication Dispensed	As a Denver Health Employee, I need the ability to dispense a specific amount of medication for a patient so that the patient has the correct number of pills dispensed.	Should Have	Out-of-the-Box	eMAR	TechCare's eMAR is used for medication administration. There are fields available to document how many pills were dispensed if a medication is KOP for DOT. If DOT, TechCare's eMAR automatically documents the administration of the equivalent of one dose. The dispense quantity of a medication is calculated at the point of medication entry in TechCare in relation to quantity, sig + duration of medication.
6.5	Functional	Medication Reconciliation	As a Denver Health Employee, I need the ability to reconcile a patients medication record so that I can determine if a patient has missed their medications.	Should Have	Out-of-the-Box	Missed Med Reporting	TechCare's eMAR has out of the box functionality to support medical staff beyond their med passes. This is in the form of a built-in missed medication report to reconcile those patients that missed pill call/pass and catch any documentation errors that could have occurred during the med pass.
6.6	Functional	Medication Disposition	As a Denver Health Employee, I need the ability to disposition a patients medication so that I can determine if a patient has taken, refused, is/was at a court appearance, or at a hospital appointment and didn't take their medication.	Should Have	Out-of-the-Box	eMAR	The eMAR is also used to document whether a medication was refused, patient no-showed, was out of facility (i.e. at court), KOP medication delivered, etc. in addition to standard medication administration.
6.7	Functional	Print Rx	As a Denver Health Employee, I need the ability to print a prescription for a patient so that the patient is able to take their prescription to any pharmacy to have it filled.	Should Have	Out-of-the-Box	Print Order	TechCare has a print order button on medication orders. This functionality prints the prescription with the ordering Provider's digital signature.
6.8	Functional	ADAP Enrollment	As a Denver Health Employee, I need the ability to mark a patient is enrolled in ADAP (Aids Drug Assistance Program) so that the Pharmacist can get the patient specific medications from an outside pharmacy and in the future you can easily identify that the patient is enrolled in the ADAP program.	Should Have	With Configuration	Flags / Drug Order Entry Parameters	With minimal configuration, this need can be accomplished. Patient charts can be easily flagged as being participants in the program and, likewise, a checkbox included on Drug Order Entry, which could signify to TechCare which fulfilling pharmacy should be sent/process the order (i.e. internal / external pharmacies).
6.9	Functional	Medication Request	As a Denver Health Employee, I need the ability to request medication if it is not in stock so that the medication or a substitution can be ordered for the patient.	Should Have	Out-of-the-Box	Stock Medication Order Form / Queue	TechCare has a stock medication ordering queue that can be used when medication stock is needed. For patient-specific medications, orders typically flow to the fulfilling pharmacy software (whether internal or external) in order to aid in medication being on hand when needed.
7	**Functional**	**DSHS Provider Workflow**	**The DSHS Health Services Providers access the patient portal so that KITE/Patient Health Care Requests can be made, appointments can be scheduled and daily schedules can be pulled.**				
7.1	Functional	KITE/Patient Health Care Request	As a Denver Health Employee, I need the ability to enter a KITE/Patient Health Care Request so that the request can be triaged and the patient will be evaluated within 24 hours.	Should Have	Out-of-the-Box	Appointment Scheduler	Sick calls are easily entered within TechCare by staff that review and triage the KITES. Depending on if the KITES are provided by inmates on paper or via kiosk, there are other means to help alleviate the manual entry of these as well. For example, patient could enter their request via kiosk or tablet > they flow automatically to a triage bucket in TechCare > triaging staff schedules the patient appropriately.
7.2	Functional	Alert	As a Denver Health Employee, I need the ability to set alerts when a workflow has exceeded a deadline, or a portion of a form is incomplete, or a patient diverts their medication, or a chart is missing a signature so that we can be made aware of outstanding tasks. (e.g. 24 hour KITE/Patient Health Care Request)	Should Have	Out-of-the-Box	Nurses Queue / Providers Queue / Others	TechCare contains multiple queues to keep these types of workflow within deadline. Additionally, if items fall out of deadline, many of the queues and worklists will add a visual trigger such as turning the line item red.
7.3	Functional	Provider Schedule Review	As a Denver Health Employee, I need the ability to pull up the provider schedule so that I can identify the patients that need to be escorted for appointments. PHI and non-PHI schedule lists will be printed.	Should Have	Out-of-the-Box	Appointment / Sick Call Viewer	The Appointment / Sick Call Viewer has the capability to print the filtered list for clinical use and a "Print for Officer" option, which removes any PHI/HIPAA information to facilitate patients being escorted to the clinic. The same "Print for Officer" functionality exists in other areas of TechCare as well, particularly the UM Queue which facilitates appointments for patients out of the facility.

ID	Requirement Type	Requirement Name	Requirement Description	MoSCoW Value	Requirement Compliance	Product/Module	Vendor Response
7.4	Functional	Forms	As a Denver Health Employee, I need the ability to fill out forms, including provider, infectious disease, dental, etc. forms so that patient information is documented in their medical chart and that there is a record of the patients exam and any follow up that is needed (it is assumed that the vendor has these forms in the system). The key difference between a form and screen in this context is that the former is typically a separate artifact from the application while the latter is typically embedded in the application. However, they typically provide similar functions (e.g. capturing input from the user to be used in a process).	Should Have	Out-of-the-Box	TechCare Forms	TechCare screenings and forms are used synonymously in most cases. There are 50+ out of the box screenings and forms built in (intake screenings, detox screenings, Mental Health screening, as well as Dental encounter forms, Chronic visit encounter forms, Psych Progress Note forms, etc.).
7.5	Functional	Flag	As a Denver Health Employee, I need the ability to flag and document a chart so that the nurses or unit clerks are notified to transcribe orders, place a patient on an internal hold, determine if a Benzo tapper is needed, and other medical alerts.	Should Have	Out-of-the-Box	Alerts	Any chart item can be referenced and sent via alert to the Nurses Queue (and other queues) as a means to solicit other user input. For example, a provider progress note can be referenced and sent as an alert for the Nurses to review and enter medications described within if the Provider did not go ahead and write them orders during the time of encounter.
8	**Functional**	**DSHS Psych Positive Screen Line Intake Process**	**DSHS Intake Health Services Providers screen patients so that a patients mental health history can be determined and they are advised of treatment(s) needed.**				
8.1	Functional	Mental Health Assessment	As a Denver Health Employee, I need the ability to complete a mental health assessment for each patient so that we can determine if a patient needs to return, needs additional medication or any further care (the assessment needs to be done within 14 days of intake).	Should Have	Out-of-the-Box	Booking / Intake Queue > Mental Health Screening	The booking queue is essential a digital checklist of all items that have to be performed for each patient entering the facility. It also is time-based so that all things are accomplished within the expected amount of time (i.e. 14 days).
8.2	Functional	Internal Hold	As a Denver Health Employee, I need the ability to create a flag/alert in JMS and an internal hold in the EHR so that a patient is not released to the street without a safety evaluation.	Should Have	Out-of-the-Box	TechCare Flags	HOLD flags exist out-of-the-box for charts and, with configuration, these can flow to the JMS system to prevent manual entry in both TechCare and JMS.
9	**Functional**	**Scheduler Workflow**	**The DSHS Scheduler workflow provides access to patient records so that they are able to refer patients to other medical providers, schedule appointments, view patient history, and communicate with other systems.**				
9.1	Functional	Clinic Referral Log	As a Denver Health Employee, I need the ability to schedule and view the clinic referral log so that we can see a list of patients that are being referred to an outside provider and I can determine if a patient needs mobility assistance when being transferred.	Should Have	Out-of-the-Box	Utilization Management (UM) Queue / Off-Site Process	The UM queue is used for management of all things for patients being referred out of the facility. It pulls in certain flag data from charts to aid in recognition of patients that will need assistance vs. staff having to view each chart individually. There is a transportation button to aid communication / list pulling for custody transportation needs.
9.1.1	Functional	Referral Form	As a Denver Health Employee, I need the ability to complete a referral form so that I can update the clinic log for the patients appointment coordination.	Should Have	Out-of-the-Box	Off-Site / Consult Order Entry	Off-Site / Consult Order Entry from a button on the patient's main chart. This funnels the request to the UM queue to be worked through the approval process and onto the scheduling of the appointment and ultimately transport and completion of the appointment to the consulting specialist.
9.2	Functional	CCMF (Correctional Care Medical Facility) Communication	As a Denver Health Employee, I need the ability to fill out the transfer form and view referral requests to CCMF at Denver Health so that the Scheduler at Denver Health CCMF can schedule the patients appointment for the requested clinic or provider.	Should Have	Out-of-the-Box	Off-Site / Consult Order Entry	Off-Site / Consult Order Entry from a button on the patient's main chart. This funnels the request to the UM queue to be worked through the approval process and onto the scheduling of the appointment and ultimately transport and completion of the appointment to the consulting specialist.
9.3	Functional	Specialty Appointments	As a Denver Health Employee, I need the ability to document and schedule appointments where a patient has their outside appointments (Denver Health or University Hospital) so that patients who have already had ongoing care established at a different facility. Ex: Oncology/cancer patients, dialysis, etc. are able to continue with their care.	Should Have	Out-of-the-Box	Utilization Management (UM) Queue / Off-Site Process	The UM module also allows for management of recurring appointments (i.e. as in the case of ongoing oncology appointments).
9.4	Functional	Sheriff Communication	As a Denver Health Employee, I need the ability to email/communicate with the sheriff's distribution list so that transportation can be coordinated for patients outside the jail and any special needs can be accommodated.	Should Have	With Configuration	Daily Report Sender	With configuration, TechCare's daily report sender can automatically pull and send transfer needs to custody for those patients that need to leave the facility in the next day, week, etc.
9.5	Functional	Schedule Appointment	As a Denver Health Employee, I need the ability to schedule a specific exam (i.e. dental exam, follow up appointments, etc.) or appointment so that a patient can receive medical services (e.g. dental exams, infectious disease specialist). If a patient is suicidal they are automatically scheduled to acute line and RFC (Recommendation For Classification) form is completed.	Should Have	Out-of-the-Box	Appointments / Sick Calls / Admissions Management	These appointments are easily made with a few clicks of a button from the patient's chart. Additionally, many appointments are added automatically based on answers to screenings and forms or at timed intervals (i.e. annual and routine exams in terms of Dental, annual physicals, PPD plants/reads, etc.). Suicidal patients are documented upon in the Admissions Management module for time based frequency/safety checks.
9.5.1	Functional	Auto Schedule Appointments	As a Denver Health Employee, I need the ability to auto schedule medical appointments (routine medical, dental, psychiatric, etc. exams) so that a patient can receive their routine care exams.	Should Have	Out-of-the-Box	Appointments / Sick Calls	Annual physicals and dental appointments are auto-scheduled when a patient enters the facility and has their initial Receiving Screening completed. Thereafter a queue displays those patients that are due within 30 days for their next physical.

Non-Functional Requirements

ID	Requirement Type	websites- ADA compliance	Requirement Description	MoSCoW Value	Requirement Compliance	Product/Module	Vendor Response
1	**Non-Functional**	**Extensibility**	**Extensibility defines the capability for the system to alter functionality generally without the need for recompiling and typically via mechanisms accessible to the customer/user.**				
1.1	Non-Functional	Workflow Management	The solution shall have the ability to automate processes executed manually for the business. It will provide an infrastructure to setup, execute, and monitor workflows.	Must Have	Out-of-the-Box	Intake, Utilization Management, Admissions Management Queue and Programs (workflow engine)	TechCare's Intake, Utilization Management, Admissions Management, and Programs workflow engines offer multiple, configurable workflow options right out of the box.
1.1.1	Non-Functional	Assign Referrals	The solution shall have the ability to automatically assign referrals and/or prompt to auto create within the workflow to a specific person.	Must Have	Out-of-the-Box	Forms	TechCare supports the automatic assignment of both internal and external referrals. The application also has the ability to prompt users for the manual or automatic creation of referrals within workflows.
1.1.2	Non-Functional	Auto Generate Referrals	The solution shall have the ability to auto-generate a referral if one is needed.	Must Have	Out-of-the-Box	Forms	TechCare supports the automatic creation of both internal and external referrals.
1.1.3	Non-Functional	Pharmacy Choice	The solution shall have the ability to choose a specific pharmacy based on location criteria (i.e. zip code, address, city, etc.).	Should Have	Out-of-the-Box	Dashboard >Pharmacies	All local pharmacies are loaded into the TechCare EHR, and can be selected during medication order entry. This is a living list of pharmacies, that can be easily maintained by authorized end-users.
1.1.4	Non-Functional	Change Status of Workflow	The solution shall have the ability to select a workflow as active or inactive.	Must Have	Out-of-the-Box	Programs >Program Administration	The TechCare EHR allows authorized end-users to set a workflow's status to active, or inactive
1.1.5	Non-Functional	Comments	The solution shall have the ability to make notations, comments, etc., during the workflow process.	Must Have	Out-of-the-Box	Intake, Utilization Management, Admissions Management Queue and Programs (workflow engine)	TechCare's Intake, Utilization Management, Admissions Management, and Programs workflow engines support notations, comments, etc. during workflow processes via associated forms, progress notes, and/or workflow specific comment fields.
1.1.6	Non-Functional	Create/modify workflow	The solution shall provide the capability for an end-user to create/modify workflow processes.	Must Have	Out-of-the-Box	Programs >Program Administration	TechCare allows authorized end-users to create/modify workflow processes.
1.1.7	Non-Functional	Escalation	The solution shall have the capability to automatically escalate to next person for review based on time limitations.	Must Have	Out-of-the-Box	Alerts	TechCare supports automatic escalation to the next person for review based on time limitations.
1.1.8	Non-Functional	Timers	The solution shall have the ability to create conditions such as timers to a workflow process (i.e. KITE/Patient Health Care Request 24 hrs*).	Must Have	Out-of-the-Box	Appointments and Reports	TechCare supports the creation and tracking of "KITE/Patient Health Care Request 24*hours ", and includes reporting options for compliance monitoring.
1.1.9	Non-Functional	Triggers	The solution shall have the ability to create triggers to skip unneeded steps or start a workflow process.	Must Have	Out-of-the-Box	Intake, Utilization Management, Admissions Management Queue and Programs (workflow engine)	The TechCare application supports the creation of triggers to skip unneeded steps or start a workflow process.
1.2	Non-Functional	Documents	The solution shall provide the ability to upload document and picture (.doc, .pdf, .jpeg, etc.) files using a mobile device and/or desktop.	Should Have	Out-of-the-Box	Scanned Documents	TechCare allows end-users to upload document and picture (.doc, .pdf, .jpeg, etc.) files using a mobile device and/or desktop.
1.3	Non-Functional	Fields	The solution shall provide the ability to make fields editable, required, locked, read-only, and/or hidden.	Could Have	Out-of-the-Box	Admin >Form Designer	TechCare's built-in form designer allows authorized end users to make fields editable, required, locked, read-only, and/or hidden.
1.4	Non-Functional	Bypassing	The solution shall provide the ability for the administration team to bypass fields.	Should Have	Out-of-the-Box	Admin >Form Designer	TechCare's built-in form designer allows authorized end users to make fields editable, required, locked, read-only, and/or hidden.
1.5	Non-Functional	Attributes	The solution shall have the ability to support user-configurable attributes/values.	Must Have	Out-of-the-Box	Admin >Settings >Configuration	TechCare's robust configuration module allows authorized users to view/modify user-configurable attributes/values.
1.6	Non-Functional	Auto-populate fields	The solution shall provide the ability to auto-populate field (i.e. one occupancy to another) within screens.	Should Have	Out-of-the-Box	Forms, Intake, Utilization Management, Admissions Management Queue and Programs (workflow engine)	Modules and forms within the TechCare EHR are fully integrated, allowing information to auto-populate into fields/queues/modules (i.e. one occupancy to another) across the application.
1.7	Non-Functional	Business Rules Management	The solution shall have the ability to create/modify key business rules. (i.e., this would include modifying the patients records to reflect medications that may have been used in the past.)	Should Have	Out-of-the-Box	eMAR	TechCare supports the import and/or manual entry of historical medication information.
1.8	Non-Functional	Common library	The solution shall have the ability to maintain a common library of reusable objects, templates, workflows and code.	Should Have	Out-of-the-Box	TechCare EHR	TechCare was created and is maintained using Microsoft's .Net libraries and C# programming language. Chosen for it's security, efficiency, and universal compatibility with nearly all computer workstations and software operating systems in use today.
1.9	Non-Functional	Dashboard	The solution shall provide the ability to customize dashboards based on user profile settings. (i.e. schedule at a glance, list of patients, medications, etc.).	Should Have	Out-of-the-Box	User Administration, Role Administration	TechCare relies Role Based Access Control (RBAC) standards present in every modern software systems. Applying those philosophies one step further for Corrections, TechCare allows not only entire roles to see different schedules at a glance, list of patients, medications, etc., but also individuals. For example, all nurses should be able to see pill call / med pass worklists, but the Charge Nurse can also see the Missed Med Report.

Non-Functional Requirements

ID	Requirement Type	websites- ADA compliance	Requirement Description	MoSCoW Value	Requirement Compliance	Product/Module	Vendor Response
1.10	Non-Functional	Email	The solution shall have the ability to email patient records, invoices, labs, referrals to any external source and maintain record of that email. (Needs the ability to email multiple individuals at one time.). (Data needs to be encrypted)	Must Have	Out-of-the-Box	Queues >Clinical Messaging (Direct Messaging)	TechCare's integrated clinical direct messaging allows authorized users to securely email patient records, invoices, labs, referrals to multiple individuals. The system maintains record of all messages sent or received via clinical direct messaging.
1.11	Non-Functional	Electronic Faxing	The solution shall have the ability to electronically fax patient information to staff, other physicians, etc. (Data needs to be encrypted).	Must Have	Out-of-the-Box	Integrated Faxing	TechCare's integrated fax functionality allows authorized users to securely fax patient information to staff, other physicians, etc.
1.12	Non-Functional	Auto-generate reports	The solution shall have the ability to automatically schedule generation and distribution of report(s) via email. (Should have the ability to schedule a report. It would be nice to have it emailed.).	Should Have	Out-of-the-Box	Daily Report Sender	The TechCare application supports automatic generation and distribution of report(s) via email.
1.13	Non-Functional	Filtering in Reports/Searches	The solution shall provide the ability to filter columns/rows in any search or report.	Should Have	Out-of-the-Box	Reports	TechCare allows users to filter columns/rows in search and report results.
1.14	Non-Functional	Monitor process	The solution shall have the ability to instantly check the status of any item to see where the bottlenecks are forming and get an estimated completion time.	Must Have	Out-of-the-Box	Intake, Utilization Management, Admissions Management Queue, Programs (workflow engine), Sick Calls, eMAR	The TechCare EHR employs a queue based approach, which allows users to easily view backlog by area. Queue-specific timers are used throughout the application to track patient length of stay (LOS) and due date of next visit, interaction, observation, etc..
1.15	Non-Functional	Personalized Correspondence	The solution shall provide the capability to customize and generate personalized customer correspondence with account information. (i.e., this would include the capability to personalize the content of bills, generate informational letters, and create customized letters for referrals, etc..) (Data needs to be encrypted)	Should Have	Out-of-the-Box	Forms and Form Designer	TechCare will be configured to display Denver County's logos, facility addresses, etc. on all printed documents. The contents of TechCare forms can be modified by authorized end-users using the applications built in form designer.
1.16	Non-Functional	e-signature	The solution shall have the capability to have an electronic signature embedded anywhere within the system especially within documents.	Must Have	Out-of-the-Box	Forms	The TechCare EHR utilizes embedded electronic signatures throughout the application, e.g. embedded within documents, modules. TechCare fully supports integrated and external signature capture methods (touch screens, signature pads, etc.)
1.17	Non-Functional	Printing	The solution should have the ability to print patient labels (i.e. lab work) and a patients entire chart in chronological order and/or print any document or any specific part of the chart.	Must Have	Out-of-the-Box	Diagnostics >Lab Order Management Print All Records	TechCare allows users to print patient labels (i.e. lab work) and a patients entire chart in chronological order and/or print any document or any specific part of the chart.
1.18	Non-Functional	Reporting formats	The solution shall have reports available in multiple formats and/or can be exported into Excel, PDF, and Word.	Should Have	Out-of-the-Box	Reports - Export/Print to PDF	The TechCare EHR allows authorized users to export report and search results for easy data manipulation in MicroSoft Excel, PDF, Word, CSV files, text files, etc.
1.19	Non-Functional	Save reports	The solution shall have the ability to save reports so that they can be re-used with only having to fill in date range instead of all report criteria so that you are able to create, run and print reports faster.	Should Have	Out-of-the-Box	Reports and Power BI Integration	TechCare allows users to to save reports so that they can be re-used with only having to fill in date range instead of all report criteria so that you are able to create, run and print reports faster.
1.20	Non-Functional	Standard and Ad-Hoc Reporting	The solution shall have the standard and ad hoc report writer which allows reporting and/or searches on any data field collected. (For example, this would include the capability to create reports using Crystal Reports, Oracle Business Intelligence Enterprise Edition(OBIEE) solutions, or comparable products.).	Must Have	Out-of-the-Box	Reports -> Ad Hoc Tool	TechCare natively includes Power BI dashboards like those highlighted below. NaphCare's dedicated BI and AI reporting teams actively create dashboards that are both scalable across our partnerships, but also specific to each County based on provided requirements. Further, we welcome the opportunity to work with our BI expert counterparts within the County to jointly develop and deploy meaningful dashboards. Finally, we continue to support data warehouse contributions. HEALTH SERVICES AT-A-GLANCE - Provides statistical information about the patient population for the current month and the previous month. The previous month will be displayed in gray on charts where the comparative statistics are displayed REAL-TIME COMPLIANCE REPORTING Displays information on the number of completed receiving screenings, physical assessments, mental health screenings, and TB screenings during a given day in relation to the number of intakes within the specific time frame, as well as the average wait time for each. The report also includes a booking process detail showing which patients are current for screenings and which are overdue for specific screenings. IMPROVED AD-HOC REPORTING TOOLS TechCare includes improved ad-hoc reporting capabilities, allowing the administration to build and

ID	Requirement Type	websites- ADA compliance	Requirement Description	MoSCoW Value	Requirement Compliance	Product/Module	Vendor Response
							customize reports based on desired information. Reports are created with scheduling, billing, or clinical information combinations by selecting data from any field of information stored within the system. Using the reworked Advanced Search tool, staff are able to “drill down” from electronic reports to view the actual data used to compile the reports, including specifics such as dates, housing locations, inmate status, etc.
1.21	Non-Functional	Tab	The solution shall allow the ability use the "tab" button in order to navigate through the forms quickly.	Must Have	Out-of-the-Box	Forms	
1.22	Non-Functional	Templates	The solution shall provide the ability to create and save different types of templates in the system for reuse. (i.e. Intake forms, Patient Medication check lists, templates for body of email, etc.)	Must Have	Out-of-the-Box	Templates and Form Designer	Additionally we provide the base SQL statements themselves in a user friendly and portable way to facilitate use in any 3rd party erpoting systems including Crystal Reports.
1.23	Non-Functional	Unique identifier for Patients	The solution shall have the ability to auto create and track a unique identifier for the each patient so that they no longer have to be tracked manually avoiding errors.	Must Have	Out-of-the-Box	Patient Ribbon (JMS number)	The TechCare application requires a unique identifier for each patient; the JMS number from the jail management system is used to identify patients in the EHR.
1.24	Non-Functional	Duplicate Appointments	The solution shall not allow for duplicate appointments in the system.	Should Have	Out-of-the-Box	Appointments	The application does not allow users to create duplicate appointments within a specified (configurable) time-frame.
2	**Non-Functional**	**Security**	**Security is the capability of a system to prevent malicious or accidental actions outside of the designed usage, and to prevent disclosure or loss of information. A secure system aims to protect assets and prevent unauthorized modification of information.**				
2.1	Non-Functional	Data Encryption	The solution shall have all City data and end user data encrypted in transmission (including via web interface) and in storage. Applications must secure data in transit using the TLS 1.2 protocol or newer. Moreover, endpoints shall not support TLS 1.1 or older or any weak ciphers.	Must Have	Out-of-the-Box	Data Encryption	The TechCare application and all interfaces utilize the TLS 1.2 protocol.
2.2	Non-Functional	Encryption	The solution shall support the FIPS 140-2 Encryption protocol.	Must Have	Out-of-the-Box	Data Encryption	The TechCare application and underlying data storage utilize FIPS 140-2 Encryption Protocol.
2.3	Non-Functional	Federated Authentication	The solution shall support federated authentication using the SAML 2.0.	Must Have	Out-of-the-Box	SSO	TechCare fully supports federated authentication using SAML 2.0
2.4	Non-Functional	DMARC	The solution shall support domain-based message Authentication, Reporting & Conformance (DMARC) using Proofpoint.	Must Have	With Configuration	Automated Email	TechCare supports DMARC authentication protocols for automated messages originating from the EHR application. Initial configuration is required for proper setup.
2.5	Non-Functional	Identity Management	The solution shall have the ability to provision users, assign them into role/groups, and manage their access rights to specific areas of the solution.	Must Have	Out-of-the-Box	Admin >Permissions	TechCare's granular, role-based permission allow the provisioning of users, assignment of users into role/groups, and management of user access rights to specific areas of the solution.
2.6	Non-Functional	Access Management	The solution shall have Access Management: This includes the features and capabilities to support Single Sign On (SSO), authentication, authorization, auditing, policy administration. The solution needs to meet the current CCD standards.	Must Have	With Configuration	Access and Authorization	TechCare is compatabile with all major SSO providers to support authentication, authorization, auditing, policy administration solutions. Initial configuration is required for setup.
2.7	Non-Functional	Role-Based Security	The solution shall have the ability to limit access to data, screens, and critical functions based on roles levels/areas of access and usage can be set by accessing user profiles in the Administrative interface.	Must Have	Out-of-the-Box	Admin >Permissions Admin >User Permissions >Patient Restrictions Admin >User Permissions >Flag Restrictions	TechCare's granular, role-based permissions module allows system administrators to limit access to data, screens, and critical functions based on roles levels/areas of access and usage can be set by accessing user profiles in the Administrative interface. In addition, TechCare allows chart-level access restrictions based on specific patient, e.g., high-profile, and/or patient flags/alerts.
2.8	Non-Functional	Audit Logging	The solution must record user activity for security and auditing purposes. The solution shall have the ability to track changes made in the solution such as who, what, and when the change was made. We need to be able to see the history of the transactions.	Must Have	Out-of-the-Box	Admin >User Review Admin >Patient Review	TechCare's robust logging records all user activity. The application tracks changes made in the solution such as who, what, when, and where (computer name and IP address) the change was made. This information can be easily viewed by authorized users via in-application menus.
2.9	Non-Functional	Authentication	The solution shall require participants and plan sponsors to use multi-factor authentication for online access to utilize the City and County of Denver's enterprise -level authorization and authentication technology and services. i.e. Active Directory (AD).	Must Have	Out-of-the-Box	2FA	TechCare integrates with Active Directory (AD), and supports 2FA.
3	**Non-Functional**	**Privacy/Data Protection**	**Privacy and data protection relates to how PII is used throughout the information lifecycle (creating, accessing, using, modifying, storing, and archiving/destroying). Privacy and data protection standards require the implementation of physical, technical and administrative safeguards to protect data throughout the information lifecycle. Compliance to standards, regulations (state and federal), and best practices must be validated and verified.**				

Non-Functional Requirements

ID	Requirement Type	websites- ADA compliance	Requirement Description	MoSCoW Value	Requirement Compliance	Product/Module	Vendor Response
3.1	Non-Functional	Personal Identifiable Information (PII)	NIST Special Publication 800-122 defines PII as "any information about an individual maintained by an agency, including (1) any information that 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, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information" as outlined in the *2_1_4_CCD ECM - Technical_Architecture_Questionnaire.docx* and *2_1_6_CCD ECM - TS_Architecture_Standards.pdf*. PII under the definition used by the National Institute of Standards and Technology: - Full name (if not common) - Home address - Email address (if private from an association/club membership, etc.) - National identification number - Passport number - IP address (when linked, but not PII by itself in US) - Vehicle registration plate number - Driver's license number - Face, fingerprints, or handwriting - Credit card numbers - Digital identity - Date of birth - Birthplace - Genetic information - Telephone number - Login name, screen name, nickname, or handle - JMS ID	Must Have	Out-of-the-Box	TechCare EHR	TechCare meets the NIST 800-122 requirements with every data export or feed from/to the system. NaphCare also conducts audits annually to confirm compliance with NIST 800-122
3.2	Non-Functional	Personal Financial Information (PFI)	Any financial information about an individual maintained by an agency, including (1) any information that 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, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, JMS ID, and employment information.	Must Have	Out-of-the-Box	TechCare EHR	TechCare protects all personally identifiable financial information. As an ONC Certified Complete EHR, it also adheres to NCCHC and ACA standards.
3.3	Non-Functional	Protected Health Information (PHI)	The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes. Learn more about protected health information at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html	Must Have	Out-of-the-Box	TechCare EHR	TechCare protects all personally identifiable health information. As an ONC Certified Complete EHR, it also adheres to NCCHC and ACA standards.
3.4	Non-Functional	National Institute of Standards and Technology (NIST) SP 800-53R4	The solution complies with the National Institute of Standards and Technology (NIST) SP 800-53R4.	Must Have	Out-of-the-Box	TechCare EHR	NaphCare has succesfully audited against SOC 2, Type II specifically as it relates to implementation and adhereance to NIST 800-53 standards within our application.
3.5	Non-Functional	Criminal Justice Information Services Division (CJIS) Security Policy	The solution complies with the Criminal Justice Information Services Division (CJIS) Security Policy. Any private or sensitive information gathered by local, state, and federal law enforcement agencies. https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view	Must Have	Out-of-the-Box	TechCare EHR	TechCare securely stores CJIS data while adhering to protection, permissions and encryption of that data. TechCare meets the CJIS requirements with every data export or feed from/to the system. NaphCare also conducts yearly audits annually to confirm compliance with NIST 800-122.
3.6	Non-Functional	Health Insurance Portability and Accountability Act (HIPAA)	The solution complies with the Health Insurance Portability and Accountability Act (HIPAA). Agreement to the regulation and safeguard requirements, acting as a Business Associate under a Business Associate Agreement (BAA).	Must Have	Out-of-the-Box	TechCare EHR	TechCare protects all personally identifiable health information, and is fully HIPAA compliant. As an ONC Certified Complete EHR, it also adheres to NCCHC and ACA standards.

Non-Functional Requirements

ID	Requirement Type	websites- ADA compliance	Requirement Description	MoSCoW Value	Requirement Compliance	Product/Module	Vendor Response
3.7	Non-Functional	National Commission on Correctional Healthcare (NCCHC)	The mission of the National Commission on Correctional Health Care is to improve the quality of health care in jails, prisons and juvenile confinement facilities. NCCHC establishes standards for health services in correctional facilities, operates a voluntary accreditation program for institutions that meet those standards, produces resource publications, conducts educational conferences and offers certification for correctional health professionals. NCCHC is supported by the major national organizations representing the fields of health, mental health, law and corrections. Each supporting organization has named a liaison to the NCCHC board of directors to create a robust, multidisciplinary governing structure that reflects the complexities of correctional health care. https://www.ncchc.org/	Must Have	Out-of-the-Box	TechCare EHR	TechCare is an an ONC Certified Complete EHR, and fully implements the standards of NCCHC with semi-annual reviews. A vast majority, over 90 percent of the facilities using TechCare, successfully attest to NCCHC including Maricopa County, AZ (8,000 ADP), NCCHC Facility of the Year.
3.8	Non-Functional	Americans with Disabilities Act (ADA)	The Americans with Disabilities Act (ADA) prohibits discrimination against people with disabilities in several areas, including employment, transportation, public accommodations, communications and access to state and local government' programs and services. As it relates to employment, Title I of the ADA protects the rights of both employees and job seekers. The ADA also establishes requirements for telecommunications relay services. Title IV, which is regulated by the Federal Communications Commission (FCC), also requires closed captioning of federally funded public service announcements.	Must Have	Out-of-the-Box	Admissions Management Reports	TechCare is an an ONC Certified Complete EHR, and is fully ADA compliant, with built-in tools and modules to drive compliance. TechCare's built-in compliance reports provide verifable compliance data.
3.9	Non-Functional	American Correctional Association (ACA)	The American Correctional Association provides a professional organization for all individuals and groups, both public and private that share a common goal of improving the justice system. https://www.aca.org	Must Have	Out-of-the-Box	Booking Queue	As an ONC Certified Complete EHR, TechCare fully implements the standards of ACA with ongoing reviews. Multiple TechCare customers successfully attest to ACA standards every year. TechCare's built-in compliance reports provide verifable compliance data.
3.10	Non-Functional	Prison Rape Elimination Act (PREA)	The Prison Rape Elimination Act (PREA) of 2003 requires that federal, state and local correctional facilities maintain and enforce a zero-tolerance policy toward sexual assault for both patient-on-patient and staff-on-patient misconduct. https://nij.ojp.gov/topics/articles/prison-rape-elimination-act	Must Have	Out-of-the-Box	Receiving Screening, Prea Rapid Risk Assessment (AK DOC), Prea Risk Assessment (NH DOC), Sexual Risk Assessment Checklist (NH DOC), Flags	TechCare utilizes multiple forms, flags, etc. in conjuncation with queues and reporting to ensure PREA patients receive appropriate, verifiable care.
3.11	Non-Functional	Data Ownership	The solution maintains that the City and County of Denver and Denver Health have ownership for any information or record in vendor product and can get a report out of their data at any time.	Must Have	Out-of-the-Box	TechCare EHR	The City and County of Denver and Denver Health have ownership for any information or record in the TechCare EHR, and may obtain a report out of their data at any time.
3.12	Non-Functional	Data Storage	The solution will ensure that the data storage is based in the US. City data must never be transferred outside of the US for processing or storage.	Must Have	Out-of-the-Box	Hosted Servers	All TechCare storage is based in the US. City data must never be transferred outside of the US for processing or storage.
4	**Non-Functional**	**Availability**	**Availability defines the proportion of time that the system is functional and working. It can be measured as a percentage of the total system downtime over a predefined period. Availability will be affected by system errors, infrastructure problems, malicious attacks, and system load.**				
4.1	Non-Functional	High Availability	Solution shall be functional and working 24 hours a day and 7 days a week. Because 99% of all business is completed between 6 am and 6pm, there is flexibility in updates happening at night. So it should function 24/7 95% of the time with 5% saved for updates happening at night.	Must Have	Out-of-the-Box	High Availability	TechCare's server architechture includes redundancies and fail-over logic that ensure the application is funcational and accesible 24 hours a day and 7 days a week. System updates can be scheduled for any time of day or night.
4.2	Non-Functional	Disaster Recovery	The software can re-establish its level of performance and recover the data directly affected in the case of a failure.	Must Have	Out-of-the-Box	Disaster Recovery	TechCare's server architechture includes redundancies, disaster recovery, off-site backups, and fail-over logic that ensure the application does not experience loss of service, or data.
4.3	Non-Functional	Downtime	The software can re-establish its level of performance and recover the data directly affected in the case of the system being down.	Must Have	Out-of-the-Box	Downtime	TechCare's server architechture includes redundancies, disaster recovery, off-site backups and fail-over logic that ensure the application does not experience loss of service, or data.
4.4	Non-Functional	Uptime	Solution shall be functional and working 24 hours a day and 7 days a week.	Must Have	Out-of-the-Box	Updtime	TechCare's server architechture includes redundancies and fail-over logic that ensure the application is funcational and accessible 24 hours a day and 7 days a week.
4.5	Non-Functional	Planned Outage	CCD shall be notified of all planned outages for any system or function of any system in advance of said outage. The minimum notification the City shall receive is 72 hours; needs to be coordinated with City services and other systems that could be impacted.	Must Have	Out-of-the-Box	Planned Outage	CCD will be notified of all planned outages for any system or function of any system in advance of said outage. Naphare will provide notification at leaset 72 hours; needs to be coordinated with City services and other systems that could be impacted.

Non-Functional Requirements

ID	Requirement Type	websites- ADA compliance	Requirement Description	MoSCoW Value	Requirement Compliance	Product/Module	Vendor Response
5	**Non-Functional**	**Interoperability**	**Interoperability is the capability of a system or different systems to operate successfully by communicating and exchanging information with other external systems written and run by external parties. An interoperable system makes it easier to exchange and reuse information internally as well as externally.**				
5.1	Non-Functional	Web Services	The solution can efficiently and effectively support data exchange (sending/receiving) using established Web Services standards/Open API (all interfaces are detailed and documented in the IRM).	Must Have	Out-of-the-Box	Interfaces	TechCare interfaces efficiently and effectively support data exchange (sending/receiving) using established Web Services standards/Open API.
6	**Non-Functional**	**Manageability**	**Manageability defines how easy it is for system administrators to manage the application, usually through sufficient and useful instrumentation exposed for use in monitoring systems and for debugging and performance tuning.**				
6.1	Non-Functional	Fault Discovery and Remediation	The solution provider can easily find and fix faults within the software system and has a sound maintenance process to support changes. If the system needs to be taken down the vendor needs to work with the City prior to any outages.	Must Have	Out-of-the-Box	Support and Maintenance	NaphCare provides a convenient online customer portal to efficiently record and track issue requests in a timely manner. This portal is available to the City 24/7. In addition, the TechCare knowledgebase is available allowing a direct link from a concern to a documented solution. While usually the purview of DSD leadership, the portal is available to anyone DSD so designates. The portal provides the following options
6.2	Non-Functional	QA Testing	Changes to the solution can be efficiently and effectively tested in a non-production environment.	Must Have	Out-of-the-Box	Regression Testing	All application changes undergo rigorous internal testing, and full regression testing is performed internally prior to every software release. In addition, a non-production test environment is provided, so that the County end users can test changes and perform regression testing prior to deployment to the production environment.
6.3	Non-Functional	Possible Upgrades	Proposed solution shall be capable of upgrading to possible future operating systems as the City updates.	Must Have	Out-of-the-Box	OS Upgrades/Web-based platform	As a flexible web-based platform that is compatible with, but not limited to, Edge, Chrome, Firefox, etc, TechCare can be utilized with any OS (Windows, IOS, Android, etc.) that supports these browsers.
6.4	Non-Functional	Expandable	The proposed solution and cost structure shall allow the capability of expanding features and capabilities in the future.	Must Have	Out-of-the-Box	Expandable (Feature Requests)	All pre-go-live application customizations are included at no additional charge. Additionally, any post-go-live upates that are made to the application to meet NCCHC, etc. requirements are provided at no additional charge.
7	**Non-Functional**	**Performance**	**Performance is an indication of the responsiveness of a system to execute any action within a given time interval. It can be measured in terms of latency or throughput. Latency is the time taken to respond to any event. Throughput is the number of events that take place within a given amount of time.**				
7.1	Non-Functional	Processing Times	The solution response, processing times and throughput rates, when performing its functions, meets requirements and shall have a response time of no longer than 1 second.	Must Have	Out-of-the-Box	TechCare EHR	The TechCare Performance Monitoring Dashboard measures system responsiveness in milliseconds, not seconds. This includes time taken to ferry puts and gets from the browser or end user workstations through the County's network to the web, application, and database servers. This process allows NaphCare's IT Systems teams to identify bottelecks and tune each link in the chain accordingly.
7.2	Non-Functional	Storage Capacity	The solution can store the necessary record volume to support business processes.	Must Have	Out-of-the-Box	Storage Capacity	The TechCare EHR utilizes the latest versions of SQL Server, and will have no issue storing the necessary record volume to support business processes.
8	**Non-Functional**	**Scalability**	**Scalability is capability of a system to either handle increases in load without impact on the performance of the system, or the capability to be readily enlarged.**				
8.1	Non-Functional	Load	The system can handle load increases without decreasing performance.	Must Have	Out-of-the-Box	System Load and Performance	The TechCare system's scalable architecture ensures a stable, consistent user experience, even during periods of heavy usage.
9	**Non-Functional**	**Recoverability**	**Recoverability refers to the capability to restore your deployment to the point at which a failure occurred. The capability to recover quickly from a system failure or disaster depends not only on having current backups of your data, but also on having a predefined plan for recovering that data on new hardware.**				
9.1	Non-Functional	Disaster Recovery	The software can re-establish its level of performance and recover the data directly affected in the case of a failure.	Must Have	Out-of-the-Box	Disaster Recovery	TechCare's server architechture includes redundancies, disaster recovery, off-site backups, and fail-over logic that ensure the application does not experience loss of service, or data.
9.2	Non-Functional	Fail Safe	The solution shall have a fail safe which will prohibit the system from ever going down.	Must Have	Out-of-the-Box	Fail Safe	TechCare's server architechture includes redundancies, disaster recovery, off-site backups, and fail-over logic that ensure the application does not experience loss of service, or data.
10	**Non-Functional**	**Usability**	**Usability defines how well the application meets the requirements of the user and consumer by being intuitive, easy to localize and globalize, providing good access to users with a variety of skills, and resulting in a good overall user experience.**				

Non-Functional Requirements

ID	Requirement Type	websites- ADA compliance	Requirement Description	MoSCoW Value	Requirement Compliance	Product/Module	Vendor Response
10.1	Non-Functional	Web UX/UI	The CCD has a set of Web UX/UI standards and guidelines that can be referenced. Refer to https://denvergov.org/denverstyleguide/.	Must Have	Out-of-the-Box	TechCare Web UX/UI	TechCare is designed with the user in mind, utilizing common UI elements, many of which are present in the CCD Web UX/UI standards.
10.2	Non-Functional	Responsive UI	Web Applications must meet responsive design standards which detects users' screens and adjusts the layout based on the screen size and orientation (example; does the application render using a modern browser or smartphone).	Must Have	Out-of-the-Box	TechCare UI	The TechCare UI has been extensively tested across all common devices, e.g., PC/Mac, tablets, smartphones
11	**Non-Functional**	**Data Retention**	**Data Retention encompasses the retention of digital and hardcopy artifacts and media. This would include the policies that define how much historical information will be available in the system and in what conditions this information will be archived/removed.**				
11.1	Non-Functional	Retention Standards	Recommend that we capture Denver's data retention standards to use as a starting point. The charts need to be retained for 10 years starting at the time of incarceration plus the age of majority which is 18.	Must Have	Out-of-the-Box	Data Retention	TechCare complies to all National, State, and/or County data retention standards.
11.2	Non-Functional	Delete/Archive	The ability to archive and/or delete data in accordance to city standards. (based user security roles)	Must Have	Out-of-the-Box	Delete/Archive	TechCare supports data archiving based on National, State, and/or County data retention standards.
12	**Non-Functional**	**Compliance**	**Compliance includes conforming to rules, such as a specification, policy, standard or law. This includes standards and guidelines as set by City and County of Denver Technology Services.**				
12.1	Non-Functional	Compliance	The solution needs to conform to the rules, policies, standards and laws as set forth by CCD and Denver Health. This includes standards and guidelines as set by City and County of Denver Technology Services.	Must Have	Out-of-the-Box	TechCare EHR	NaphCare successfully completed our SOC II, Type II Audit in parallel with the release of v.5 of TechCare further ensuring our commitment to a reliable, secure experience. NaphCare maintains a detailed, well maintained IT Security Plan which covers NaphCare as a company, our datacenters/IT Resources, and our partners including CCD/DSD. As NaphCare, acting as a custodian of CCD data in a hosted environment, we have committed to several standards of IT security to protect that data including: • COBIT – Control Objectives for Information Technology • FedRAMP – Federal Risk and Authorization Management Program • FISMA – Federal Information Security Act • HIPAA – Health Insurance Portability and Accountability Act • NIST 800 – National Institute of Standards and Technology • SAS 70 –Statement on Auditing Standards
12.2	Non-Functional	websites- ADA compliance	All websites should be ADA WCAG 2.0 compliant and in 2024 will need to be ADA WCAG 2.1 compliant.	Must Have	Out-of-the-Box	TechCare EHR	TechCare is WCAG 2.0 compliant and will be WCAG 2.1 Level AA compliant.
12.3	Non-Functional	Order forms/documents - ADA compliance	All order sheets or any documentation should be ADA WCAG 2.0 compliant and in 2024 will need to be ADA WCAG 2.1 compliant	Must Have	Out-of-the-Box	TechCare EHR	TechCare is WCAG 2.0 compliant and will be WCAG 2.1 Level AA compliant.
13	**Non-Functional**	**Compatibility**	**Compatibility defines the devices that the external system needs to be able to work with in order to function within our environment.**				
13.1	Non-Functional	Tablet	The software needs to be compatible with IPAD, Android or Windows tablets.	Must Have	Out-of-the-Box	Tablet Use	TechCare is compatible with tablets running Windows OS, Android OS and/or iPads (IOS)
13.2	Non-Functional	Mobile	The mobile app should provide all the functionality that the web based application does, unless we restricted the features for any reason.	Must Have	Out-of-the-Box	TechCare EHR	There are no differences in presentation or funcationality of the TechCare EHR when used on a mobile device. All screens are responsive to scaling and usability.

Transition Requirements

ID	Requirement Type	Requirement Name	Requirement Description	MoSCoW Value	Requirement	Product/Module	Vendor Response
1	**Transition**	**Data Migration**	**Captures the data migration requirements necessary to transition from the current solution to the new solution. This could include requirements such as data mapping, data cleanup/verification, data transfer (extraction/loading), and any other testing to ensure for a successful data migration.**				
1.1	Transition	Data Migration	The solution needs to allow for a dual system of the new system and the ability to scan in charts as needed.	Must Have	Out-of-the-Box	Patient Main Screen > Attach Documents	NaphCare includes a robust Data Migration plan as presented in b.4 #15 Data Migration in our RFP response. Further, the system supports scaning of records directly from the patient main screen with a simple Attach Documents link/button and the capability to use drag and drop functionality. This enables a dual system approach as required.
2	**Transition**	**System Migration**	**Captures the system migration requirements necessary to transition from the current solution to the new solution. This could include requirements such as orchestrating the cutover, special testing/validation, and any other requirements necessary to ensure a successful system migration.**				
2.1	Transition	System Availibility	The solution has to have a plan in place to cut over to new system with minimal downtime.	Must Have	Out-of-the-Box	Data Migration Plan / Go-Live Plan	Our GoLive plan is fully presented in Phase 4 Deployment and Go Live section of our 4 phased deployment plan within our RFP response. With every implementation, we worked with the client to plan Cutover (go-live) activities. The idea is to 'flip a switch' and be operational with all data migration activities occurring in the weeks/days leading up to go-live. There is no 'downtime' in terms of migrating the data in prior to users having the ability to login. Our proven processes have succesfully enables facilities using paper or electronic sytsem to move to TechCare seamlessly, without impact to patient care.
2.2	Transition	API interaction	The solution shall provide Data and Technology the needed API access so they have the ability to integrate other systems with this new solution.	Must Have	Out-of-the-Box	Integration Development	TechCare has an out-of-the-box API solution available for many data items within TechCare to include: demographics, alerts, diets, clinical diagnostics, appointments, etc. Each interface is deployed following the plan presented in XXX.
2.3	Transition	Integrations	The solution shall provide the capability to test and deploy multiple complex system integrations. Including mapping exercises. Please see the IRM for further information.	Must Have	Out-of-the-Box	Integration Development	Our approach to integration including project strategies, testing, and deployment is further explained in B.4 #7 Interface Strategy and detailed within the IRM as requested.
3	**Transition**	**Support**	**Captures the requirements necessary so that there is adequate resources and processes in place for ongoing support (e.g. help desk, etc.).**				
3.1	Transition	Service Level Agreement (SLA)	The solution shall have the ability to meet the SLA. Please review section B.1.d of the RFP for the Service Level Agreement (SLA) document prior to responding this requirement.	Must Have	Out-of-the-Box	NaphCare 24/7 IT Support and Support Portal	NaphCare's standard SLA exceeds that required by the RFP. We will meet the requested SLA as defined.
3.2	Transition	Online Support	The solution shall have 24*7 Self service online support center (Chat, FAQs, Log incident, etc.).	Must Have	Out-of-the-Box	NaphCare 24/7 IT Support and Support Portal	TechCare's support team is available 24/7. Additionally, the support portal contains many Knowledge Base articles, along with an online User Manual. Additional Details can be found in B.4 # 13 B in our RFP response.
3.3	Transition	Email Support	The solution shall have 24*7 Email support.	Must Have	Out-of-the-Box	NaphCare 24/7 IT Support and Support Portal	Should the online support portal be unailable, NaphCare support team can be reached by email at support@naphcare.com.
3.4	Transition	Phone Support	The solution shall have standard business day telephone support.	Must Have	Out-of-the-Box	NaphCare 24/7 IT Support	TechCare's support team is staffed 24/7 with live, at the desk telephone support from NaphCare FTEs.
3.5	Transition	GoLive Support	The solution shall have a go-live support plan of 60 business days or 3 months in place. This is a period of time post implementation that the vendor is available to address any identified issues.	Must Have	Out-of-the-Box	SWAT Team / Go-Live Readiness	NaphCare provides 'at-the-elbow' support of clinical users on the ground during go-live activities. Additionally, a post-go-live support/grace period exists for feature adjustment where necessary.
4	**Transition**	**Training**	**Captures the training requirements necessary to use and maintain the new solution. This would include training requirements such as onsite, online, "train-the-trainer", and any other training as deemed necessary by the stakeholders.**				
4.1	Transition	Online Tutorial	The solution shall include permanent online trainings (not live).	Must Have	Out-of-the-Box	TechCare Online User Manual / Video Library	TechCare has an online user manual in addition to each facility receiving an online tailored version with specifics to their TechCare installation alone. Additionally, there is an online library of helpful TechCare tutorials. The manual is also printable. Additional Details can be found in B.4 # 13 B in our RFP response.
4.2	Transition	Train the Trainer	The solution shall include a train the trainer.	Must Have	Out-of-the-Box	Super User Training	Super User Training occurs ahead of standard end user training where TechCare "Super Users" learn TechCare back to front. Our approach to training is further defined in section B.4 # 16 System Training in our RFP response..
4.3	Transition	Train the Team	The solution shall include a train the team session.	Must Have	Out-of-the-Box	End User Training	End User Training typically occurs 1-2 weeks ahead of go-live and is role/discipline based as in Nursing Sessions, Dental Sessions, Pharmacy and Provider-Specific Sessions. NaphCare will directly train all end-users by NaphCare FTE trainers. Additional Details can be found in B.4 # 16 System Training in our RFP response.

Transition Requirements

ID	Requirement Type	Requirement Name	Requirement Description	MoSCoW Value	Requirement	Product/Module	Vendor Response
4.4	Transition	Live webinar training	The solution shall include live online (webinar) training/refresher available.	Must Have	Out-of-the-Box	Ongoing Virtual Training Events	TechCare holds multiple online virtual training events each year as further detailed in B.4 # 16 Training in our RFP response.
4.5	Transition	Testing	The solution shall include system testing prior to implementation and training. Vendor shall work with the CCD team on use cases for testing.	Must Have	Out-of-the-Box	Implementation Plan / UAT Plan	System and UAT are included with every implementation, to include sharing of use and test cases for the clinical users / Denver team involved in system testing.
5	**Transition**	**Documentation**	**Captures the documentation requirements necessary to use and maintain the new solution. This would include document requirements such as user and administrative documentation, hardcopy and electronic artifacts, knowledge base, and other documentation as deemed necessary by the stakeholders.**				
5.1	Transition	User Guides	The solution shall have electronic and hard copy user guides based on the different roles identified.	Must Have	Out-of-the-Box	TechCare Online User Manual / Video Library	TechCare has an online user manual in addition to each facility receiving an online tailored version with specifics to their TechCare installation alone. Additionally, there is an online library of helpful TechCare tutorials. The manual is also printable and available in PDF format. Reference material which is role specific is also provided.
5.2	Transition	Manuals	Online user manuals for future reference.	Must Have	Out-of-the-Box	TechCare Online User Manual / Video Library	TechCare has an online user manual in addition to each facility receiving an online tailored version with specifics to their TechCare installation alone. Additionally, there is an online library of helpful TechCare tutorials. The manual is also printable and available in PDF format.
5.3	Transition	Upgrades	Supply electronic documentation instructions for upgrades if you have any available.	Must Have	Out-of-the-Box	Technical Handoff Instructions	Technical Handoff Instructions are provided to client IT departments for any involvement needed (if any) on their end. TechCare handles the upgrade process on a bimonthly basiss with 6 releases per year. Each release is fully supported by NaphCare include change management control that aligns with your processes and schedules. Additional Details can be found in B.4 # 13 B in our RFP response..
6	**Transition**	**Licensing**	**Captures requirements on the type of licenses, cost, reissuance, and other factors of licensing. Licensing requirements are often driven by the budgetary constraints of the business and technology stakeholders.**				
6.1	Transition	Business Licenses	The solution shall have licenses based on the different roles identified; internal versus external.	Must Have	Out-of-the-Box	TechCare EHR	NaphCare provides an unlimited County license that includes unlimited users, roles, providers, patients, charts, facilities, etc. The license cost is fixed throughout the contract period.
6.2	Transition	Open Source	System should be open source or free version. This needs to be maintained and supported for the life of the product. Patching needs to be done on a regular basis.	Must Have	Out-of-the-Box	TechCare EHR	The core TechCare application is not open source/free. However, some underlying technologies supporting healthcare integration do follow an open source license. Such tools are industry standard (i.e. Mirth Connect). For these cases, we will comply with this requirement.
6.3	Transition	Java	If Oracle Java is proposed and going to be used, support must be purchased and maintained for the life of the product. It needs to be patched on a regular basis.	Must Have	Out-of-the-Box	TechCare EHR	Java is NOT utilized within TechCare currently. There are no plans to utilize Java, however we will comply with this requirement should this position change.
7	**Transition**	**Warranty**	**Captures requirements on warranties (e.g. Hardware, Software, Services) and the remediation related to the warranty (e.g. hardware replacement, monetary reimbursement, etc.)**				
7.1	Transition	Security Issues	The solution shall guarantee that all security issues be identified, addressed and resolved with the City and County of Denver TS.	Must Have	Out-of-the-Box	TechCare EHR Services	NaphCare maintains a robust security stance with well defined policy and processes. We comply with the following standards and maintain SOC II Type 2 comliance. Additional information on our security stance can be found in Approach to System Security on pag 39 of our RFP response.
7.2	Transition	Warranty Period	The solution shall include a warranty period that aligns with the CCD standards.	Must Have	Out-of-the-Box	TechCare EHR Services	NaphCare services compliy with the CCD standards as presented.

RequirementCompliance	Description
Cannot Meet	The product cannot meet the requirement “Out-of-the-Box”, “With Configuration”, “With Custom Programming” or with a “Future Release”.
Future Release	The current version of the solution cannot meet the requirement “Out of the Box” or “With Configuration” but will be able to with a scheduled, future release of the product.
Out-of-the-Box	The solution meets the requirement as is, “out-of-the-box” functionality with no configuration or custom programming/coding.
With Configuration	The solution can meet the requirement by arranging the functional parameters that are already inherent in the product – and not by changing the product’s source code – so that it functions in a way that meets the City’s specific business needs.
With Custom Programming	The solution can meet the requirement only by modifying the product’s source code (changing or adding new code) to enable it to do what it was not originally able to do.

Prioritization Type	Prioritization Description
Must Have	Requirements labeled as "Must Have" are critical to the current delivery timebox in order for it to be a success. If even one "Must Have" requirement is not included, the project delivery should be considered a failure (note: requirements can be downgraded from "Must Have", by agreement with all relevant stakeholders; for example, when new requirements are deemed more important).
Should Have	Requirements labeled as "Should Have" are important but not necessary for delivery in the current delivery timebox. While "Should Have" requirements can be as important as "Must Have", they are often not as time-critical or there may be another way to satisfy the requirement, so that it can be held back until a future delivery timebox.
Could Have	Requirements labeled as "Could Have" are desirable but not necessary, and could improve user experience or customer satisfaction for little development cost. These will typically be included if time and resources permit.
Won't Have	Requirements labeled as "Won't Have" have been agreed by stakeholders as the least-critical, lowest-payback items, or not appropriate at that time. As a result, "Won't Have" requirements are not planned into the schedule for the next delivery timebox. "Won't Have" requirements are either dropped or reconsidered for inclusion in a later timebox. (Note: occasionally the term Would like to have is used; however, that usage is incorrect, as this last priority is clearly stating something is outside the scope of delivery)

Exhibit C Integration Requirements Matrix

ID	Transaction Type	Source	Description	Candidate Integration Mechanism	Event/Trigger	Volume	Security Constraints	MoSCoW Value	Requirement Compliance	Product/Module	Vendor Response Comments
1	**Jail Management Records**	**ATIMS-JMS**	**Integration provides data for target system's jail management functionality (Approximately 2,300 inmates are in custody each year at the Denver Detention Center (DDC) and Denver County Jail (DCJ)). DSD has web API's for searching and retrieving current account information from JMS-ATIMS and sending them to the current system. Data flow is just one direction.**	**Web Services**	**Real-Time**	**Dependent on the jail population and demands of visitations being scheduled.**	**Subject to data protection requirements. (HIPPA, PII, Protected, Sensitive, Regulated or Confidential data).**	**Must Have**	**Out-of-the-Box**	TechCare EHR - JMS Plug-in (Intergration Engine)	TechCare has experience interfacing with ATIMS, with multiple interfaces between our systems in use today. We understand that the requirement is for one way communication, however, many of our integrations with ATIMS support bi-directional information sharing capabilities.
1.1	Application Access	User initiates request to connect to the application (e.g. hyperlink). This supports the overarching requirement that the EHR Solution act as centralized portal for the users.		Web Services	Real-Time	Dependent on the jail population and demands of visitations being scheduled.	Subject to data protection requirements. (HIPPA, PII, Protected, Sensitive, Regulated or Confidential data).	Must Have	**Out-of-the-Box**	TechCare EHR - JMS Plug-in (Intergration Engine)	TechCare is capable of initiating requests to connect to the application (e.g. hyperlink). While all current integrations with ATIMS are completely seamless (i.e. all data shared between systems is displayed in the correct format to the user directly within the application), TechCare is also capable of providing a hyperlink to the ATIMS application for easy access. Further, TechCare being a fully web-based solution makes the user experience seamless.
1.2	Data Exchange	The EHR Solution would initiate a request to perform data exchanges between systems. This would require invoking web services on ATIMS-JMS if real-time processing is required.		Web Services	Real-Time	Dependent on the jail population and demands of visitations being scheduled.	Subject to data protection requirements. (HIPPA, PII, Protected, Sensitive, Regulated or Confidential data).	Must Have	**Out-of-the-Box**	TechCare EHR - JMS Plug-in (Intergration Engine)	TechCare is capable of initiating a request to perform data exchanges with ATIMS, invoking web services on ATIMS as real-time processing is required. This is TechCare's preferred method of communication with ATIMs.
2	**Health System Records**	**EPIC**	**Integration provides data for target system's medical and behavioral health data for patients. EHR to EHR clinical information interfaces are typically used between two clinical systems looking to exchange patient-specific information. They include both the transport standards for clinical information exchange and the format and content of the information exchanged. Data flow is just one**	**Web Services**	**Real-Time**	**Dependent on the jail population.**	**Subject to data protection requirements. (HIPPA, PII, Protected, Sensitive, Regulated or Confidential data).**	**Must Have**	**Out-of-the-Box**	TechCare EHR - Clinical Exchange Plug-in (Intergration Engine)	TechCare has experience interfacing with EPIC to exchange clinical information in real time. This is achieved with the utilization of CCD documentsion and EPIC's CareEverywhere platform which TechCare natively integrates with. TechCare follows the HL7 FHIR standard for interoperability, allowing increased communication and efficiency between TechCare and other systems such as HIEs, hospitals, etc. Additionally, with v5.0, TechCare has achieved the latest Health IT certification (Cures Act) by the Office of the National Coordinator for Health Information Technology (ONC-HIT).
2.1	Application Access	Ability to leverage API from conent aware links or FHIR APIs that can log a user into a system with single sign on and look up a patient.		Web Services	Real-Time	Dependent on the jail population.	Subject to data protection requirements. (HIPPA, PII, Protected, Sensitive, Regulated or Confidential data).	Must Have	**Out-of-the-Box**	TechCare EHR	TechCare's APIs are are capable of leveraging conent aware links or FHIR APIs to log a user into a system using single sign on and automatically look up a patient. From an end user perspective, this would allow the opening of an EPIC chart directly from the TechCare EHR application without added clicks.
2.2	Patient History Lookup	System initiates request to connect to the application (e.g. hyperlink). This supports the overarching requirement that the EHR Solution act as centralized work portal for the users.		Web Services	Real-Time	Dependent on the jail population.	Subject to data protection requirements. (HIPPA, PII, Protected, Sensitive, Regulated or Confidential data).	Must Have	**Out-of-the-Box**	TechCare EHR	TechCare is capable of initiating requests to connect to the application (e.g. hyperlink). While all current integrations with EPIC are completely seamless (i.e. all data shared between systems is displayed in the correct format to the user directly within the appliaction), TechCare is also capable of providing a hyperlink to the EPIC application for easy access. Further, TechCare being a fully web-based solution makes the user experience seamless.

Integration Requirements

ID	Transaction Type	Source	Description	Candidate Integration Mechanism	Event/Trigger	Volume	Security Constraints	MoSCoW Value	Requirement Compliance	Product/Module	Vendor Response Comments
2.3	Data Exchange	The EHR Solution would initiate a request to perform data exchanges between systems. This would require invoking web services on EPIC if real-time processing is required. https://open.epic.com/Clinical/EHRtoEHR		Web Services	Real-Time	Dependent on the jail population.	Subject to data protection requirements. (HIPPA, PII, Protected, Sensitive, Regulated or Confidential data).	Must Have	**Out-of-the-Box**	TechCare EHR - Clinical Exchange Plug-in (Intergration Engine)	TechCare is capable of initiating a request to perform data exchanges between systems, and can invoke web services on EPIC. TechCare utilizes Incoming Patient Discovery, Outgoing Patient Discovery, XDS.b, Direct Messaging, and CDA to achieve these items all of which are compatible with the standards on open.epic.com.
2.4	Laboratory Orders and Results	HL7 integration to support the workflows between system and Denver Health. https://open.epic.com/Tech/TechSpec?spec=staged%2FOutgoing%20Results%20and%20Orders%20Interface%20Technical%20Specification.zip		Web Services	Real-Time	Dependent on the jail population.	Subject to data protection requirements. (HIPPA, PII, Protected, Sensitive, Regulated or Confidential data).	Must Have	**Out-of-the-Box**	TechCare EHR - Diagnostic Exchange Plug-in (Intergration Engine)	TechCare's HL7 integration is capable of fully supporting laboratory orders and results workflows with Denver Health and EPIC. We maintain proven interoperability with EPIC in similar deployments.
2.5	Radiology Orders and Results	HL7 Interfaces to support the workflows between system and Denver Health. https://open.epic.com/Tech/TechSpec?spec=staged%2FOutgoing%20Imaging%20Results%20and%20Orders%20Interface%20Technical%20Specification.pdf		Web Services	Real-Time	Dependent on the jail population.	Subject to data protection requirements. (HIPPA, PII, Protected, Sensitive, Regulated or Confidential data).	Must Have	**Out-of-the-Box**	TechCare EHR - Diagnostic Exchange Plug-in (Intergration Engine)	TechCare's HL7 integration is capable of fully supporting radiology orders and results workflows with Denver Health and EPIC. We maintain proven interoperability with EPIC in similar deployments.
2.6	Outpatient Prescriptions	HL7 Interfaces to support the workflows between system and Denver Health. https://open.epic.com/Ancillary/Pharmacy		Web Services	Real-Time	Dependent on the jail population.	Subject to data protection requirements. (HIPPA, PII, Protected, Sensitive, Regulated or Confidential data).	Must Have	**Out-of-the-Box**	TechCare EHR - Medication Exchange Plug-in (Intergration Engine)	TechCare's HL7 integration is capable of fully supporting prescription medication order workflows with Denver Health and EPIC.
2.7	Closed Loop Referrals	HL7 Interfaces to support the workflows between system and Denver Health via clinical direct messaging. https://open.epic.com/Clinical/EHRtoEHR		Web Services	Real-Time	Dependent on the jail population.	Subject to data protection requirements. (HIPPA, PII, Protected, Sensitive, Regulated or Confidential data).	Must Have	**Out-of-the-Box**	TechCare EHR - Direct Messaging	TechCare's maintains out of the box functionality for integrated direct messaging and is capable of fully supporting workflows with Denver Health across this standard. Our Direct Messaging platform comes fully configured with a HISP supporting connectivity to the national database of direct messaging recipients.
2.8	Transtions of care summaries	Create, transmit, recieve and ingest Clinical Document Architecture (CDAs) via national interoperability standards for the purposes of transitions of care. https://open.epic.com/Home/InteroperabilityGuide?whoAmI=provider&whatIWant=externalHealthRecord		Web Services	Real-Time	Dependent on the jail population.	Subject to data protection requirements. (HIPPA, PII, Protected, Sensitive, Regulated or Confidential data).	Must Have	**Out-of-the-Box**	TechCare EHR - C-CDA	TechCare's Clinical Messages Queue, Discharge Release Summary, and custom implemetation of REST and FHIR APIs all can create, transmit, recieve and ingest Clinical Document Architecture (CDAs) via national interoperability standards for the purposes of transitions of care.
3	**Federated Authentication for SSO**	**Active Directory**	**Supports federated authentication using the SAML, OAUTH, or OpenID protocol.** **This allows city users to use their network username/password to login to the solution.** **Data flow is just one**	**XML**	**Real-Time**	**Users of the system**	**Subject to data protection requirements. (HIPPA, PII, Protected, Sensitive, Regulated or Confidential data).**	**Must Have**	**Out-of-the-Box**	TechCare EHR - SAML/OAuth	TechCare supports federated authentication using the SAML, OAUTH, or OpenID protocols
3.1	Authentication	Use multi-factor authentication for online access to the participant website.		XML	Real-Time	Users of the system	Subject to data protection requirements. (HIPPA, PII, Protected, Sensitive, Regulated or Confidential data).	Must Have	**Out-of-the-Box**	TechCare EHR - 2FA	TechCare supports 2FA solutions which may already be deployed by Denver (i.e. Okta, RSA, etc.) or comes pre-loaded with 2FA technology using token codes and mobile devices.
3.2	Federated Authentication	Use federated authentication using the SAML 2.0 protocol.		XML	Real-Time	Users of the system	Subject to data protection requirements. (HIPPA, PII, Protected, Sensitive, Regulated or Confidential data).	Must Have	**Out-of-the-Box**	TechCare EHR - SAML/OAuth	TechCare fully supports federated authentication using SAML 2.0
3.3	Role-Based Security	Access to data, screens, and critical functions can be limited based on roles.		XML	Real-Time	Users of the system	Subject to data protection requirements. (HIPPA, PII, Protected, Sensitive, Regulated or Confidential data).	Must Have	**Out-of-the-Box**	TechCare - User Permissions	TechCare's granular, role-based permissions module allows system administrators to limit access to data, screens, and critical functions based on roles levels/areas of access and usage can be set by accessing user profiles in the Administrative interface. In addition, TechCare allows chart-level access restrictions based on specific patient, e.g., high-profile, and/or patient flags/alerts.

Integration Requirements

ID	Transaction Type	Source	Description	Candidate Integration Mechanism	Event/Trigger	Volume	Security Constraints	MoSCoW Value	Requirement Compliance	Product/Module	Vendor Response Comments
4	**State of Colorado Immunization Registry**	**State of Colorado Immunization Registry**	**The Colorado Immunization Information System (CIIS) is a lifelong immunization record tracking system under the Colorado Immunization Registry Act of 2007.** **CIIS has signed agreements with all participating sites that are authorized to provide information to or access information from CIIS. CIIS and all people and entities that access immunization records are required to maintain the confidentiality of those records.**	**Web Services**	**Real-Time** **Initiated by a query in the Enterprise Cashiering System (ECS).**	**REVISIT - This number will greatly depend on the number of the Users in the TBD Wastewater Billing/CRM Solution and the volume of work performed.**	**Subject to data protection requirements. (HIPPA, PII, Protected, Sensitive, Regulated or Confidential data).**	**Should Have**	**Out-of-the-Box**	Immunization Registry	TechCare has experience interfacing with immuniztions registries nationwide (State of Alaska's VacTrAK, State of Califorinia's CAIR, Virginia Commonwealth's VIIS), with multiple interfaces in use today. TechCare's existing presence in the state of Colorado further exemplifies our commitment to integration with state-wide systems.
4.1	Application Access	User initiates request to connect to the application (e.g. hyperlink). This supports the overarching requirement that the EHR Solution act as centralized portal for the users.		Web Services	Real-Time Initiated by a query in the Enterprise Cashiering System (ECS).	REVISIT - This number will greatly depend on the number of the Users in the TBD Wastewater Billing/CRM Solution and the volume of work performed.	Subject to data protection requirements. (HIPPA, PII, Protected, Sensitive, Regulated or Confidential data).	Should Have	**Out-of-the-Box**	Immunization Registry	TechCare's allows users to initiate request to connect to the application (e.g. hyperlink). This supports the overarching requirement that the EHR Solution act as centralized portal for the users.
4.2	Data Exchange	The EHR Solution would initiate a request to perform data exchanges between systems. This would require invoking web services on CIIS if real-time processing is required.		Web Services	Real-Time Initiated by a query in the Enterprise Cashiering System (ECS).	REVISIT - This number will greatly depend on the number of the Users in the TBD Wastewater Billing/CRM Solution and the volume of work performed.	Subject to data protection requirements. (HIPPA, PII, Protected, Sensitive, Regulated or Confidential data).	Should Have	**Out-of-the-Box**	Immunization Registry	TechCare is capable of initiating a request to perform data exchanges with CIIS, invoking web services on CIIS if real-time processing is required. This is the preffered approach to integration.

System	Description
ATIMS-JMS	ATIMS is a SaaS provider of law enforcement and public safety software, with fully integrated solutions for self-contained or systemwide application. ATIMS systems are used by law enforcement, corrections, and justice agencies throughout the United States. ATIMS offers comprehensive jail management solutions that integrate with court systems, commissary vendors, video visitation software and more.
EPIC	EPIC is an electronic medical record (EMR)Saas software application. Epic's applications support functions related to patient care, including registering and scheduling; clinical systems for doctors, nurses, emercency personnel, and othr care providers; systems for lab technoloists, pharmacists, and radiologists; and billing systems for insurers.
Active Directory	Active Directory stores information about ojects on the network and makes this information easy for administrators and users to find and use. Active Directory uses a structured data store as the basis for a loical, hierarchial organization of directory inforamtion.
State of Colorado Immunization Registry	Also known as Colorado's immunization registry, the Colorado Immunization Information System (CIIS) is a confidential, population-based, computerized system that collects and consolidates vaccination data for Coloradans of all ages from a variety of sources. CIIS is a program within the Immunization Branch of the Colorado Department of Public Health and Environment. CIIS helps health care providers, schools, child care centers, and individuals keep track of the shots they and/or their children have received.

Prioritization Type	Prioritization Description
Must Have	Requirements labeled as "Must Have" are critical to the current delivery timebox in order for it to be a success. If even one "Must Have" requirement is not included, the project delivery should be considered a failure (note: requirements can be downgraded from "Must Have", by agreement with all relevant stakeholders; for example, when new requirements are deemed more important).
Should Have	Requirements labeled as "Should Have" are important but not necessary for delivery in the current delivery timebox. While "Should Have" requirements can be as important as "Must Have", they are often not as time-critical or there may be another way to satisfy the requirement, so that it can be held back until a future delivery timebox.
Could Have	Requirements labeled as "Could Have" are desirable but not necessary, and could improve user experience or customer satisfaction for little development cost. These will typically be included if time and resources permit.
Won't Have	Requirements labeled as "Won't Have" have been agreed by stakeholders as the least-critical, lowest-payback items, or not appropriate at that time. As a result, "Won't Have" requirements are not planned into the schedule for the next delivery timebox. "Won't Have" requirements are either dropped or reconsidered for inclusion in a later timebox. (Note: occasionally the term Would like to have is used; however, that usage is incorrect, as this last priority is clearly stating something is outside the scope of delivery)

ACORD®

Exhibit D

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY): 09/30/2024

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER VIG, LLC, The Vestavia Group 2090 Columbiana Road Ste. 2000 Birmingham AL 35216	**CONTACT NAME:** Hunter Williams **PHONE (A/C, No, Ext):** 205-266-7304 **FAX (A/C, No):** 205-244-8072 **E-MAIL ADDRESS:** hunter.williams@vestaviagroup.com
INSURED NaphCare, Inc. 2090 COLUMBIANA RD. Ste. 4000 Birmingham AL 35216	**INSURER(S) AFFORDING COVERAGE** — **NAIC #** **INSURER A :** Ironshore Insurance Company "A" XV — 25445 **INSURER B :** Arch Insurance Company "A+" XV — 11150 **INSURER C :** The Travelers Insurance Company "A++" XV — 25615 **INSURER D :** Markel Service, Incorporated "A" XV — 38970 **INSURER E :** **INSURER F :**

COVERAGES **CERTIFICATE NUMBER:** **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	[X] COMMERCIAL GENERAL LIABILITY [X] CLAIMS-MADE [ ] OCCUR Retro Date: 12/31/2018 GEN'L AGGREGATE LIMIT APPLIES PER: [ ] POLICY [ ] PRO-JECT [ ] LOC [ ] OTHER:	Y	Y	HC7BAB5A62004	12/31/2024	12/31/2025	EACH OCCURRENCE DAMAGE TO RENTED PREMISES (Ea occurrence) MED EXP (Any one person) PERSONAL & ADV INJURY GENERAL AGGREGATE PRODUCTS - COMP/OP AGG 	$ 2,000,000 $ 100,000 $ 5,000 $ 2,000,000 $ 11,000,000 $ 2,000,000 $
B	AUTOMOBILE LIABILITY [X] ANY AUTO [ ] OWNED AUTOS ONLY [ ] SCHEDULED AUTOS [ ] HIRED AUTOS ONLY [ ] NON-OWNED AUTOS ONLY	Y	Y	41CAB1078001	9/30/2024	9/30/2025	COMBINED SINGLE LIMIT (Ea accident) BODILY INJURY (Per person) BODILY INJURY (Per accident) PROPERTY DAMAGE (Per accident) 	$ 1,000,000 $ XXXXXXXX $ XXXXXXXX $ XXXXXXXX $
	[ ] UMBRELLA LIAB [ ] OCCUR [ ] EXCESS LIAB [ ] CLAIMS-MADE [ ] DED [ ] RETENTION $			Not Applicable	XXXXXXX	XXXXXXX	EACH OCCURRENCE AGGREGATE 	$ XXXXXXXX $ XXXXXXXX $
C	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANYPROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) Y/N: Y If yes, describe under DESCRIPTION OF OPERATIONS below	N / A	Y	UB-1P248768-24-51-K UB-1P250924-24-51-R	9/30/2024	9/30/2025	[X] PER STATUTE [ ] OTH-ER E.L. EACH ACCIDENT E.L. DISEASE - EA EMPLOYEE E.L. DISEASE - POLICY LIMIT	 $ 1,000,000 $ 1,000,000 $ 1,000,000
A	Professional Liability Claims Made Retro Date: 10/01/2022	N	N	HC7BAB5A62004	12/31/2024	12/31/2025	Each Med. Incident Aggregate	2,000,000 11,000,000
D	Cyber Liability/Tech. E&O	N	Y	MKLV3PEO004660	1/11/2024	1/11/2025	Occ./Agg.	$5mm/$5mm

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

Contract #: TECHS-202473962

Electronic Health Records Software Solution for Denver Sheriff's Department

It is understood and agreed the City and County of Denver, its Elected and Appointed Officials, Employees, and Volunteers shall be named as Additional Insured, as respects their contract with NaphCare, Inc. If there are material changes or modifications to any of the above policies, a thirty (30) day written notice shall be provided to the City and County of Denver.

CERTIFICATE HOLDER **CANCELLATION**

ACORD®

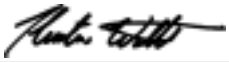
City and County of Denver Department of Technology Services 201 W. Colfax Ave. Dept. 301 Denver, CO. 80202	**SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.** **AUTHORIZED REPRESENTATIVE** 

EXHIBIT E, INFORMATION TECHNOLOGY PROVISIONS

This Exhibit regarding Information Technology Provisions (this "Exhibit") is a material part of the Agreement between the Parties to which this Exhibit is attached. In addition to the requirements of the main body of this Agreement, the Contractor shall protect the City's information technology resources and City Data in accordance with this Exhibit. All provisions of this Exhibit that refer to the Contractor shall apply equally to any Subcontractor performing work in connection with this Agreement. Unless the context clearly requires a distinction between the Agreement and this Exhibit, all references to "Agreement" shall include this Exhibit.

1. TECHNOLOGY SERVICES SPECIFICATIONS

1.1. User ID Credentials: Internal corporate or customer (tenant) user account credentials shall be restricted, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures, as follows:

- **1.1.1.** Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation);
- **1.1.2.** Account credential lifecycle management from instantiation through revocation;
- **1.1.3.** Account credential and/or identity store minimization or re-use when feasible; and
- **1.1.4.** Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expire able, non-shared authentication secrets).

1.2. Identity Management: The City's Identity and Access Management ("IdM") system is an integrated infrastructure solution that enables many of the City's services and online resources to operate more efficiently, effectively, and securely. All new and proposed applications must utilize the authentication and authorization functions and components of IdM. Strong authentication is required for privileged accounts or accounts with access to sensitive information. This technical requirement applies to all solutions regardless of where the application is hosted.

1.3. Supported Releases: The Contractor shall maintain the currency of all third-party software used in the development and execution or use of the Work with third-party vendor approved and supported releases, including, but not limited to, all code libraries, frameworks, components, and other products (e.g., Java JRE, code signing certificates, .NET, jQuery plugins, etc.), whether commercial, free, open-source, or closed-source. This includes any of the Contractor's controlled systems running on the City's network, including, but not limited to, any application, firewall, or other type of physical or virtual appliances.

1.4. Updates & Upgrades: During the Term of this Agreement, the Contractor shall provide the City with copies of all new versions, updates, and upgrades of the On-Premise Software (collectively, "Upgrades"), without additional charge, promptly after commercial release. Upon delivery to the City, Upgrades will become part of the On-Premise Software and will be subject to the license and other terms of this Agreement applicable to such On-Premise Software. In addition, the Contractor shall ensure that SaaS receives all updates and upgrades the Contractor provides to its customers generally.

1.5. **Compatibility with Third-Party Software**: The Contractor acknowledges and agrees that the Work must integrate and operate compatibly with various third-party software products. The Contractor shall actively monitor and stay current on new version releases, updates, and changes made to any such third-party software that interfaces or integrates with the Contractor's Work. The Contractor shall ensure that its own products remain fully compatible with the most recent generally available versions of these third-party software components. Within ninety (90) days of the commercial release of a new generally available version of any interfacing third-party software, the Contractor shall complete all necessary testing, coding, and product updates to certify compatibility with the new version. The Contractor shall provide the updated and version-compatible products to the City at no additional cost. If the Contractor's Work is not compatible with the most current generally available third-party software versions required for operation, the City reserves the right to temporarily cease using the incompatible Work until the compatibility issue is resolved, without penalty or payment for a period of noncompliance. Under no circumstances shall the Contractor require the City to run old, non-current versions of third-party software to remain compatible with the Contractor's Work. The responsibility and costs for ensuring third-party software version compatibility shall reside solely with the Contractor.

1.6. **Adjustment of Licenses**: The City may, at each anniversary date of this Agreement, increase or decrease the number of licenses it has purchased under this Agreement by giving written notice to the Contractor at least thirty (30) days prior to the anniversary date. The Contractor shall adjust the invoice for the next billing period based on the unit price per license specified in this Agreement. The City shall not reduce the number of licenses below the minimum quantity required under this Agreement.

1.7. **Timing of Fees and Subscriptions**: Notwithstanding any provision to the contrary: (i) no fees for maintenance of On-Premise Software or SaaS, including without limitation for Upgrades, will accrue before Go-Live (as defined below); and (ii) no period before Go-Live will be counted against the time covered by any maintenance period. In addition, no fees for use of SaaS will accrue before Go-Live, and no period before Go-Live will be counted against the time covered by any SaaS subscription fees. “Go-Live” refers to the earlier of Acceptance of the On-Premise Software or SaaS or the City’s first use of the On-Premise Software or SaaS in production, other than a beta use or trial.

1.8. **Performance Outside of the United States**: The Contractor shall request written approval from the City to perform, or subcontract to perform, Services outside the United States. The City may approve or deny such request within the City’s sole discretion. Any notice or term in any Exhibit provided to the City by the Contractor regarding performance outside the United States shall be deemed ineffective and void if the City has not granted prior written approval for such performance. This prohibition shall also apply to using, processing, transmitting, or maintaining City Data outside of the United States. Notwithstanding anything to the contrary contained in the Agreement, the City shall have no responsibility or obligation to comply with foreign data protection laws or polices, including, but not limited to, the General Data Protection Regulation of the European Union.

1.9. **Continuity of Critical Services**: The Contractor acknowledges that the Work to be performed under this Agreement is vital to the City and must be continued without interruption and that, upon this Agreement's expiration without renewal, a successor, either the City or another contractor, may continue them. The Contractor agrees to: (i) furnish phase-in training; and (ii) exercise its best efforts and cooperation to complete an orderly and efficient transition to a successor. The Contractor shall, upon the City's written notice: (i) furnish phase-in, phase-out services for up to sixty (60) days after this Agreement expires; and (ii) negotiate in good faith to determine the nature and extent of phase-in, phase-out services required. The Contractor shall provide sufficient experienced personnel during the phase-in, phase-out period to ensure that the Work called for by this Agreement is maintained at the required level of proficiency. The Contractor shall be reimbursed for all reasonable phase-in, phase-out costs (i.e., costs incurred within the agreed period after expiration that result from phase-in, phase-out operations) at the rates contained herein. The City shall have the authority extend this Agreement monthly if additional time is required beyond the termination of this Agreement, if necessary, to effectuate the transition, and the City shall pay a proration of the subscription fee during any necessary extension.

1.10. **Software Escrow**: At the City's request, the Contractor shall maintain in escrow a copy of the source code and documentation for the licensed software purchased under this Agreement. With each new release of the software provided to the City, the Contractor shall maintain the updated source code and documentation in escrow. If the Contractor files for bankruptcy, becomes insolvent, or ceases operations for any reason, the City shall be provided the current source code and documentation in escrow. The City will only use the source code and documentation to support the licensed software. This Section shall survive the termination of this Agreement.

2. SECURITY AUDITS

2.1. **Performance of Security Audits**: Prior to the Effective Date of this Agreement, the Contractor, will at its expense conduct or have conducted the following, and thereafter, the Contractor will at its expense conduct or have conducted the following at least once per year, and immediately after any actual or reasonably suspected Security Breach: (i) a SSAE 18/SOC 2 Type 2 or other mutually agreed upon audit of the Contractor's security policies, procedures and controls; (ii) a quarterly external and internal vulnerability scan of the Contractor's systems and facilities, to include public facing websites, that are used in any way to deliver Services under this Agreement. The report must include the vulnerability, age, and remediation plan for all issues identified as critical or high; and (iii) a formal penetration test performed by qualified personnel of the Contractor's systems and facilities that are used in any way to deliver Work under this Agreement. The Contractor will provide the City the results of the above audits. The Contractor shall also protect data against deterioration or degradation of quality and authenticity by, at minimum, having a third party perform annual data integrity audits. In addition, the Contractor shall comply with the City's annual risk assessment and the results thereof.

2.2. **Security Audit Results**: The Contractor will provide the City the reports or other documentation resulting from the above audits, certifications, scans, and tests within seven (7) business days of

the Contractor's receipt of such results. The report must include the vulnerability, age, and remediation plan for all issues identified as critical or high. Based on the results and recommendations of the above audits, the Contractor will, within thirty (30) calendar days of receipt of such results, promptly modify its security measures to meet its obligations under this Agreement and provide the City with written evidence of remediation. The City may require, at the Contractor's expense, that the Contractor perform additional audits and tests, the results of which will be provided to the City within seven (7) business days of Contractor's receipt of such results. To the extent the Contractor controls or maintains information systems used in connection with this Agreement, the Contractor shall provide the City with the results of all security assessment activities when conducted on such information systems, including any code-level vulnerability scans, application-level risk assessments, and other security assessment activities as required by this Agreement or reasonably requested by the City. The Contractor will remediate any vulnerabilities to comply with its obligations hereunder. If additional funds are required to perform the tests required by the City that are not accounted for in this Agreement, the Parties agree to amend this Agreement as necessary.

3. DATA MANAGEMENT AND SECURITY

3.1. Compliance with Data Protection Laws and Policies: In addition to the compliance obligations imposed by this Agreement, the Contractor shall comply with all information security and privacy obligations imposed by any federal, state, or local statute or regulation, or by any specifically incorporated industry standards or guidelines, as applicable to the Contractor under this Agreement, including, without limitation, applicable industry standards or guidelines based on the data's classification relevant to the Contractor's performance hereunder. If the Contractor becomes aware that it cannot reasonably comply with the terms or conditions contained herein due to a conflicting law or policy, the Contractor shall promptly notify the City.

3.2. Data Ownership: Unless otherwise required by law, the City has exclusive ownership of all City Data under this Agreement, and the Contractor shall have no right, title, or interest in City Data. The Parties recognize and agree that the Contractor is a bailee for hire with respect to City Data. The Contractor's use and possession of City Data is solely on the City's behalf, and the Contractor shall only use City Data solely for the purpose of performing its obligations hereunder and shall not use City Data in the development of machine learning and artificial intelligence models for any purpose without the City's written consent. The City retains the right to access and retrieve City Data stored on the Contractor's infrastructure at any time during the Term. All City Data created and/or processed by the Work, if any, is and shall remain the property of the City and shall in no way become attached to the Work. This Agreement does not give a Party any rights, implied or otherwise, to the other's data, content, or intellectual property, except as expressly stated in this Agreement.

3.3. Data Access and Integrity: The Contractor shall implement and maintain all appropriate administrative, physical, technical, and procedural safeguards necessary and appropriate to ensure compliance with the applicable law and regulation as they relate to the Contractor's performance hereunder to ensure the security and confidentiality of City Data. The Contractor shall protect

against threats or hazards to the security or integrity of data; protect against unauthorized disclosure, access to, or use of data; restrict access to data as necessary; and ensure the proper and legal use of data. The Contractor shall provide the City with access, subject to the Contractor's reasonable security requirements, for purposes of inspecting and monitoring access and use of City Data and evaluating security control effectiveness. The Contractor shall not engage in "data mining" except as specifically and expressly required by law or authorized in writing by the City. Upon written request, the Contractor shall provide the City its policies and procedures to maintain the confidentiality of City Data.

3.4. **Response to Legal Orders for City Data**: If the Contractor is required by a court of competent jurisdiction or administrative body to disclose City Data, the Contractor shall first notify the City and, prior to any disclosure, cooperate with the City's reasonable requests in connection with the City's right to intervene, quash, or modify the legal order, demand, or request, and upon request, provide the City with a copy of its response. Upon notice, the City will promptly coordinate with the Contractor regarding the preservation and disposition of any City Data and records relevant to any current or anticipated litigation. If the City receives a subpoena, legal order, or other legal demand seeking data maintained by the Contractor, the City will promptly provide a copy to the Contractor. Upon notice and if required by law, the Contractor shall promptly provide the City with copies of its data required for the City to meet its necessary disclosure obligations.

3.5. **Mandatory Disclosures**: In addition to the requirements set forth herein, the Contractor shall provide the City with a copy of any disclosure the Contractor is required to file with any regulatory body as a result of a Security Breach or other incident that requires the Contractor to make such a disclosure, including but not limited to, required disclosures mandated by the Securities and Exchange Commission. If the contents of any such disclosure is protected by law, the Contractor shall instead provide the City with prompt notice that it was required to make such a disclosure along with the name of the regulatory body requiring the Contractor to make such a disclosure.

3.6. **Data Retention, Transfer, Holds, and Destruction**: Using appropriate and reliable storage media, the Contractor shall regularly backup data used in connection with this Agreement and retain such backup copies as necessary to meets its obligations hereunder. All City Data shall be encrypted in transmission, including by web interface, and in storage by an agreed upon National Institute of Standards and Technology ("NIST") approved strong encryption method and standard. Upon the expiration or termination of this Agreement, the Contractor shall, as directed by the City, promptly return all City Data provided by the City to the Contractor, and the copies thereof, to the City or destroy all such City Data and certify to the City that it has done so; however, this requirement shall not apply to the extent the Contractor is required by law to retain copies of certain City Data. The Contractor shall not interrupt or obstruct the City's ability to access and retrieve City Data stored by the Contractor. Unless otherwise required by law or regulation, when paper or electronic documents are no longer needed, the Contractor shall destroy or arrange for the destruction of such documents within its custody or control that contain City Data by shredding, erasing, or otherwise modifying the City Data in the paper or electronic documents to make it unreadable or indecipherable. The Contractor's obligations set forth in this Subsection,

without limitation, apply likewise to the Contractor's successors, including without limitation any trustee in bankruptcy.

3.7. **Software and Computing Systems**: At its reasonable discretion, the City may prohibit the Contractor from the use of certain software programs, databases, and computing systems with known vulnerabilities to collect, use, process, or store, City Data received under this Agreement. The Contractor shall fully comply with all requirements and conditions, if any, associated with the use of software programs, databases, and computing systems as reasonably directed by the City. The Contractor shall not use funds paid by the City for the acquisition, operation, or maintenance of software in violation of any copyright laws or licensing restrictions. The Contractor shall maintain commercially reasonable network security that, at a minimum, includes network firewalls, intrusion detection/prevention, and enhancements or updates consistent with evolving industry standards The Contractor shall use industry-standard and up-to-date security tools, technologies and procedures including, but not limited to, anti-virus and anti-malware protections. The Contractor shall ensure that any underlying or integrated software employed under this Agreement is updated on a regular basis and does not pose a security threat. Upon request, the Contractor shall provide a software bill of materials ("SBOM") annually or upon major changes to the solution(s) provided to the City under this Agreement. The Contractor shall provide a complete SBOM for the supported life of the solution(s). The Contractor shall monitor for security vulnerabilities in applicable software components and use a risk-based approach to mitigate any vulnerabilities.

3.8. **Background Checks**: The Contractor shall ensure that, prior to being granted access to City Data, the Contractor's agents, employees, Subcontractors, volunteers, or assigns who perform work under this Agreement have all undergone and passed all necessary criminal background screenings, have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all data protection provisions of this Agreement and applicable law, and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the data. If the Contractor has access to federal tax information ("FTI") under this Agreement, the Contractor shall comply with the background check requirements of IRS Publication 1075.

3.9. **Subcontractors**: If the Contractor engages a Subcontractor under this Agreement, the Contractor shall ensure its Subcontractors are subject to data protection terms that provide at least the same level of data protection as in this Agreement and to the extent appropriate to the nature of the Work provided. The Contractor shall monitor the compliance with such obligations and remain responsible for its Subcontractor's compliance with the obligations of this Agreement and for any of its Subcontractors acts or omissions that cause the Contractor to breach any of its obligations under this Agreement. Unless the Contractor provides its own security protection for the information it discloses to a third party, the Contractor shall require the third party to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the City Data disclosed and that are reasonably designed to protect it from unauthorized access, use, modification, disclosure, or destruction. Any term or condition within this Agreement relating to the protection and confidentially of any disclosed data shall apply equally to both the Contractor

and any of its Subcontractors, agents, assigns, employees, or volunteers. Upon request, the Contractor shall provide the City copies of its record retention, data privacy, and information security policies. The Contractor shall ensure all Subcontractors sign, or have signed, agreements containing nondisclosure provisions at least as protective as those in this Agreement, and that the nondisclosure provisions are in force so long as the Subcontractor has access to any data disclosed under this Agreement. Upon request, the Contractor shall provide copies of those signed nondisclosure agreements to the City.

3.10. **Request for Additional Protections and Survival**: In addition to the terms contained herein, the City may reasonably request that the Contractor protect the confidentiality of certain City Data to ensure compliance with applicable law and any changes thereto. Unless a request for additional protections is mandated by a change in law, the Contractor may reasonably decline the City's request to provide additional protections. If such a request requires the Contractor to take steps beyond those contained herein, the Contractor shall notify the City with the anticipated cost of compliance, and the City may thereafter, in its sole discretion, direct the Contractor to comply with the request at the City's expense; provided, however, that any increase in costs that would increase the Maximum Contract Amount must first be memorialized in a written amendment complying with City procedures. Obligations contained in this Agreement relating to the protection and confidentially of any disclosed data shall survive termination of this Agreement, and the Contractor shall continue to safeguard all data for so long as the data remains confidential or protected and in the Contractor's possession or control.

4. DISASTER RECOVERY AND CONTINUITY

4.1. The Contractor shall maintain a continuous and uninterrupted business continuity and disaster recovery program with respect to the Work provided under this Agreement. The program shall be designed, in the event of a significant business disruption affecting the Contractor, to provide the necessary and sufficient capabilities, processes, and procedures to enable the Contractor to resume and continue to perform its duties and obligations under this Agreement without undue delay or disruption. In the event of equipment failures, the Contractor shall, at no additional expense to the City, take reasonable steps to minimize service interruptions, including using any back-up facilities where appropriate. Upon request, the Contractor shall provide the City with a copy of its disaster recovery plan and procedures.

4.2. Prior to the Effective Date of this Agreement, the Contractor shall, at its own expense, conduct or have conducted the following, and thereafter, the Contractor will, at its own expense, conduct or have conducted the following at least once per year:

4.2.1. A test of the operability, sufficiency, and completeness of business continuity and disaster recovery program's capabilities, processes, and procedures that are necessary to resume and continue to perform its duties and obligations under this Agreement.

4.2.2. Based upon the results and subsequent recommendations of the testing above, the Contractor will, within thirty (30) calendar days of receipt of such results and recommendations, promptly modify its capabilities, processes, and procedures to meet its obligations under this Agreement and provide City with written evidence of remediation.

4.2.3. Upon request, the Contractor shall provide the City with report summaries or other documentation resulting from above testing of any business continuity and disaster recovery procedures regarding the Services provided under this Agreement.

4.3. The Contractor represents that it is capable, willing, and able to provide the necessary and sufficient business continuity and disaster recovery capabilities and functions that are appropriate for it to provide services under this Agreement.

5. DELIVERY AND ACCEPTANCE

5.1. **Acceptance & Rejection**: Deliverables will be considered accepted ("Acceptance") only when the City provides the Contractor affirmative written notice of acceptance that such Deliverable has been accepted by the City. Such communication shall be provided within a reasonable time from the delivery of the Deliverable and shall not be unreasonably delayed or withheld. Acceptance by the City shall be final, except in cases of Contractor's failure to conduct proper quality assurance, latent defects that could not reasonably have been detected upon delivery, or the Contractor's gross negligence or willful misconduct. The City may reject a Deliverable if it materially deviates from its specifications and requirements listed in this Agreement or its Exhibits by written notice setting forth the nature of such deviation. In the event of such rejection, the Contractor shall correct the deviation, at its sole expense, and redeliver the Deliverable within fifteen (15) days. After redelivery, the Parties shall again follow the acceptance procedures set forth herein. If any Deliverable does not perform to the City's satisfaction, the City reserves the right to repudiate acceptance. If the City ultimately rejects a Deliverable, or repudiates acceptance of it, the Contractor will refund to the City all fees paid, if any, by the City with respect to any rejected Deliverable. Acceptance shall not relieve the Contractor from its responsibility under any representation or warranty contained in this Agreement, and payment of an invoice prior to Acceptance does not grant a waiver of any representation or warranty made by the Contractor.

5.2. **Quality Assurance**: The Contractor shall provide and maintain a quality assurance system acceptable to the City for Deliverables under this Agreement and shall provide to the City only such Deliverables that have been inspected and found to conform to the specifications identified in this Agreement and any applicable solicitation, bid, offer, or proposal from which this Agreement results. The Contractor's delivery of any Deliverables to the City shall constitute certification that any Deliverables have been determined to conform to the applicable specifications, and the Contractor shall make records of such quality assurance available to the City upon request.

6. WARRANTIES AND REPRESENTATIONS

6.1. Notwithstanding the acceptance of any Work, or the payment of any invoice for such Work, the Contractor warrants that any Work provided by the Contractor under this Agreement shall be free from material defects and shall function as intended and in material accordance with the applicable Specifications. The Contractor warrants that any Work, and any media used to distribute it, shall be, at the time of delivery, free from any harmful or malicious code, including without limitation viruses, malware, spyware, ransomware, or other similar function or technological means designed to disrupt, interfere with, or damage the normal operation of the

Work and the use of City resources and systems. The Contractor's warranties under this Section shall apply to any defects or material nonconformities discovered within 180 days following delivery of any Work.

6.2. Upon notice of any defect or material nonconformity, the Contractor shall submit to the City in writing within 10 business days of the notice one or more recommendations for corrective action with sufficient documentation for the City to ascertain the feasibility, risks, and impacts of each recommendation. The City's remedy for such defect or material non-conformity shall be:

6.2.1. The Contractor shall re-perform, repair, or replace such Work in accordance with any recommendation chosen by the City. The Contractor shall deliver, at no additional cost to the City, all documentation required under this Agreement as applicable to the corrected Work or Deliverable; or

6.2.2. The Contractor shall refund to the City all amounts paid for such Work, as well as pay to the City any additional amounts reasonably necessary for the City to procure alternative goods or services of substantially equivalent capability, function, and performance.

6.3. Any Work delivered to the City as a remedy under this Section shall be subject to the same quality assurance, acceptance, and warranty requirements as the original Work. The duration of the warranty for any replacement or corrected Work shall run from the date of the corrected or replacement Work.

6.4. **Customization Services**: The Contractor warrants that it will perform all customization services, if any, in a professional and workmanlike manner. In case of breach of the warranty of the preceding sentence, the Contractor, at its own expense, shall promptly re-perform the customization services in question or provide a full refund for all nonconforming customization services.

6.5. **Third-Party Warranties and Indemnities**: The Contractor will assign to the City all third-party warranties and indemnities that the Contractor receives in connection with any Work or Deliverables provided to the City. To the extent that the Contractor is not permitted to assign any warranties or indemnities through to the City, the Contractor agrees to specifically identify and enforce those warranties and indemnities on behalf of the City to the extent the Contractor is permitted to do so under the terms of the applicable third-party agreements.

6.6. **Intellectual Property Rights in the Software**: The Contractor warrants that it is the owner of all Deliverables, and of each and every component thereof, or the recipient of a valid license thereto, and that it has and will maintain the full power and authority to grant the intellectual property rights to the Deliverables in this Agreement without the further consent of any third party and without conditions or requirements not set forth in this Agreement. In the event of a breach of the warranty in this Section, the Contractor, at its own expense, shall promptly take the following actions: (i) secure for the City the right to continue using the Deliverable as intended; (ii) replace or modify the Deliverable to make it non-infringing, provided such modification or replacement will not materially degrade any functionality as stated in this Agreement; or (iii) refund 100% of the fee paid for the Deliverable for every month remaining in the Term, in which case the Contractor may terminate any or all of the City's licenses to the infringing Deliverable granted in

this Agreement and require return or destruction of copies thereof. The Contractor also warrants that there are no pending or threatened lawsuits, claims, disputes, or actions: (i) alleging that any of the Work or Deliverables infringes, violates, or misappropriates any third-party rights; or (ii) adversely affecting any Deliverables or Services, or the Contractor's ability to perform its obligations hereunder.

6.7. **Disabling Code**: The Work will contain no malicious or disabling code that is intended to damage, destroy, or destructively alter software, hardware, systems, or data. The Contractor represents, warrants and agrees that the City will not receive from the Contractor any virus, worm, trap door, back door, timer, clock, counter or other limiting routine, instruction or design, or other malicious, illicit or similar unrequested code, including surveillance software or routines which may, or is designed to, permit access by any person, or on its own, to erase, or otherwise harm or modify any City system, resources, or data (a "Disabling Code"). In the event a Disabling Code is identified, the Contractor shall take all steps necessary, at no additional cost to the City, to: (i) restore and/or reconstruct all data lost by the City as a result of a Disabling Code; (ii) furnish to City a corrected version of the Work or Deliverables without the presence of a Disabling Code; and, (iii) as needed, re-implement the Work or Deliverable at no additional cost to the City. This warranty shall remain in full force and effect during the Term.

7. PAYMENT CARD INDUSTRY DATA SECURITY STANDARD COMPLIANCE

7.1. If the Contractor is directly involved in the processing, storage, or transmission of cardholder data on behalf of the City as part of this Agreement, this Section shall apply. Any contractor who provides or has access to software, systems, hardware, or devices which process and/or interact with payment card information or payment cardholder data must be compliant with the current version of the Payment Card Industry Data Security Standard (PCI DSS).

7.2. The Contractor covenants and agrees to comply with Visa's Cardholder Information Security Program (CISP), MasterCard's Site Data Protection Rules (SDP), and with all other credit card association or National Automated Clearing House Association (NACHA) rules or rules of member organizations ("Association"), and further covenants and agrees to maintain compliance with the PCI DSS, SDP, and (where applicable) the Payment Application Data Security Standard (PA-DSS) (collectively, the "Security Guidelines"). The Contractor represents and warrants that all of the hardware and software components utilized for the City or used under this Agreement is now and will be PCI DSS compliant during the term of this Agreement. All service providers that the Contractor uses under this Agreement must be recognized by Visa as PCI DSS compliant. The Contractor further agrees to exercise reasonable due diligence to ensure that all of its service providers (as defined by the PCI Security Council), agents, business partners, contractors, Subcontractors, and any third party who may have access to credit card information under this Agreement maintain compliance with the Security Guidelines and comply in full with the terms and conditions set out in this Section. The Contractor further certifies that the equipment, as described herein, will be deployed in a manner that meets or exceeds the PA DSS and/or PCI certification and will be deployed on a network that meets or exceeds PCI standards. The Contractor shall demonstrate its compliance with PCI DSS by annually providing the City an

executed Attestation of Compliance (AOC). The Contractor must provide verification to the City, prior to start up and ongoing annually during the term of this Agreement, that all modules of the Contractor's system(s) that interface with or utilize credit card information in any manner or form of collection are PCI DSS compliant. If the Contractor is a service provider involved in the processing, storage or transmission of cardholder data or sensitive authentication data (collectively "Data Handling") on behalf of the City that would result in Data Handling being included in the City's PCI scope through connected software or components, then the Contractor must provide a PCI Responsibility Matrix ("Matrix") to be attached to this Agreement as an exhibit. The Matrix must identify where responsibility resides for each PCI control requirement, whether it be with the Contractor, the City or shared by both. Any PCI control requirements that do not apply should be indicated along with any pertinent notes.

7.3. The Contractor shall not retain or store CAV2/CVC2/CVV2/CID or such data prohibited by PCI DSS subsequent to authorization of a credit card transaction, shall prohibit disclosure of any and all cardholder information, and in the event of a compromise of credit card information of any kind, the Contractor shall notify the City in writing consistent with the Security Breach response notification requirements of this Agreement, and shall provide, at the Contractor's sole expense, all necessary and appropriate notification to parties and persons affected by such disclosure and compromise.

7.4. If any Association requires an audit of the Contractor or any of the Contractor's Service Providers, agents, business partners, contractors, or Subcontractors due to a data security compromise event related to this Agreement, the Contractor agrees to cooperate with such audit. If as a result of an audit of the City it is determined that any loss of information is attributable to the Contractor, the Contractor shall pay the City's reasonable costs relating to such audit, including attorney's fees. No review, approval, or audit by the City shall relieve the Contractor from liability under this Section or under other provisions of this Agreement.

7.5. The Contractor is solely responsible for its PCI DSS compliance. The Contractor shall ensure that all PCI DSS vendors comply with PCI DSS standards: (i) in providing Services or Deliverables to the City under this Agreement; (ii) in storing, processing, or transmitting PCI data; and (iii) in engaging in any other activities for any purpose relating to this Agreement. As between the Contractor and the City, the Contractor shall be responsible for a PCI DSS vendor's non-compliance with PCI DSS.

7.6. In addition to all other defense and indemnity obligations undertaken by the Contractor under this Agreement, the Contractor, to the extent that its performance of this Agreement includes the allowance or utilization by members of the public of credit cards to pay monetary obligations to the City or the Contractor, or includes the utilization, processing, transmittal and/or storage of credit card data by the Contractor, shall defend, release, indemnify and save and hold harmless the City against any and all fines, penalties, assessments, costs, damages or other financial obligations, however denominated, assessed against the City and/or the Contractor by credit card company(s), financial institution(s) or by the National Automated Clearing House Association (NACHA) or successor or related entity, including but not limited to, any credit card company

fines, regardless of whether considered to be consequential, special, incidental or punitive damages, costs of notifying parties and persons affected by credit card information disclosure, the cost of replacing active credit cards, and any losses associated with fraudulent transaction(s) occurring after a security breach or loss of information with respect to credit card information, and shall defend, release, indemnify, and save and hold harmless the City from any and all claims, demands, suits, actions, liabilities, causes of action or legal or equitable proceedings of any kind or nature, of or by anyone whomsoever, in any way affected by such credit card data or utilizing a credit card in the performance by the Contractor of this Agreement. In furtherance of this, the Contractor covenants to defend and indemnify the City and the Contractor shall maintain compliance with PCI DSS and with all other requirements and obligations related to credit card data or utilization set out in this Agreement.

8. LICENSE OR USE AUDIT RIGHTS

8.1. To the extent that the Contractor, through this Agreement or otherwise as related to the subject matter of this Agreement, has granted to the City any license or otherwise limited permission to use any of the Contractor's intellectual property, the terms of this Section shall apply.

8.2. The Contractor shall have the right, at any time during and throughout the Term, but not more than once per year, to request via written notice in accordance with the notice provisions of this Agreement that the City audit its use of and certify as to its compliance with any applicable license or use restrictions and limitations contained in this Agreement (an "Audit Request"). The Audit Request shall specify the period to be covered by the audit, which shall not include any time covered by a previous audit. The City shall complete the audit and provide certification of its compliance to the Contractor ("Audit Certification") within a reasonable amount of time following the City's receipt of the Audit Request.

8.3. If upon receipt of the City's Audit Certification, the Parties reasonably determine that: (i) the City's use of licenses, use of software, use of programs, or any other use during the audit period exceeded the use restrictions and limitations contained in this Agreement ("Overuse"), and (ii) the City would have been or is then required to purchase additional maintenance and/or services ("Maintenance"), the Contractor shall provide written notice to the City in accordance with the notice provisions of this Agreement identifying any Overuse or required Maintenance and request that the City bring its use into compliance with such use restrictions and limitations.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

EXHIBIT F, BUSINESS ASSOCIATE AGREEMENT
HIPAA/HITECH

1. GENERAL PROVISIONS AND RECITALS.

1.01 The parties agree that the terms used, but not otherwise defined below, shall have the same meaning given to such terms under 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 their implementing regulations at 45 CFR Parts 160 and 164 ("the HIPAA regulations") as they exist or may hereafter be amended.

1.02 The parties agree that a business associate relationship (as described in 45 CFR §160.103) under HIPAA, the HITECH Act, and the HIPAA regulations arises between the CONTRACTOR and the CITY to the extent that CONTRACTOR performs, or delegates to subcontractors to perform, functions or activities on behalf of CITY.

1.03 CITY wishes to disclose to CONTRACTOR certain information, some of which may constitute Protected Health Information ("PHI") as defined below, to be used or disclosed in the course of providing services and activities.

1.04 The parties intend to protect the privacy and provide for the security of PHI that may be created, received, maintained, transmitted, used, or disclosed pursuant to the Agreement in compliance with the applicable standards, implementation specifications, and requirements of HIPAA, the HITECH Act, and the HIPAA regulations as they exist or may hereafter be amended.

1.05 The parties understand and acknowledge that HIPAA, the HITECH Act, and the HIPAA regulations do not pre-empt any state statutes, rules, or regulations that impose more stringent requirements with respect to privacy of PHI.

1.06 The parties understand that the HIPAA Privacy and Security rules apply to the CONTRACTOR in the same manner as they apply to a covered entity. CONTRACTOR agrees to comply at all times with the terms of this Agreement and the applicable standards, implementation specifications, and requirements of the Privacy and the Security rules, as they exist or may hereafter be amended, with respect to PHI.

2. DEFINITIONS.

2.01 "Administrative Safeguards" are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic PHI and to manage the conduct of CONTRACTOR's workforce in relation to the protection of that information.

2.02 "Agreement" means the attached Agreement and its exhibits to which these additional terms are incorporated by reference.

2.03 "Breach" means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI.

2.03.1 Breach excludes:

1. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of CONTRACTOR or CITY, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.

2. Any inadvertent disclosure by a person who is authorized to access PHI to another person authorized to access PHI, or organized health care arrangement in which CITY participates, and the information received as a result of such disclosure is not further used or disclosed in a manner disallowed under the HIPAA Privacy Rule.

3. A disclosure of PHI where CONTRACTOR or CITY has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

2.03.2 Except as provided in paragraph (a) of this definition, an acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule is presumed to be a breach unless CONTRACTOR demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

2. The unauthorized person who used the PHI or to whom the disclosure was made;

3. Whether the PHI was actually acquired or viewed; and

4. The extent to which the risk to the PHI has been mitigated.

2.04 "CONTRACTOR" shall have the same meaning as in the attached Agreement, to which these Business Associate terms are incorporated by reference.

2.05 "CITY" shall have the same meaning as in the attached Agreement, to which these Business Associate terms are incorporated by reference.

2.06 "Data Aggregation" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR §164.501.

2.07 "Designated Record Set" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR §164.501.

2.08 "Disclosure" shall have the meaning given to such term under the HIPAA regulations in 45 CFR §160.103.

2.09 "Health Care Operations" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR §164.501.

2.10 "Immediately" where used here shall mean within 24 hours of discovery.

2.11 "Individual" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR §160.l03 and shall include a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).

2.12 "Parties" shall mean "CONTRACTOR" and "CITY", collectively.

2.13 "Physical Safeguards" are physical measures, policies, and procedures to protect CONTRACTOR's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

2.14 "The HIPAA Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

2.15 "Protected Health Information" or "PHI" shall have the meaning given to such term under the HIPAA regulations at 45 CFR §160.103.

2.16 "Required by Law" shall have the meaning given to such term under the HIPAA Privacy Rule at 45 CFR §164.103.

2.17 "Secretary" shall mean the Secretary of the Department of Health and Human Services or his or her designee.

2.18 "Security Incident" means attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. "Security incident" does not include trivial incidents that occur on a daily basis, such as scans, "pings", or unsuccessful attempts to penetrate computer networks or servers maintained by CONTRACTOR.

2.19 "The HIPAA Security Rule" shall mean the Security Standards for the Protection of electronic PHI at 45 CFR Part 160, Part 162, and Part 164, Subparts A and C.

2.20 "Subcontractor" shall have the meaning given to such term under the HIPAA regulations at 45 CFR §160.103.

2.21 "Technical safeguards" means the technology and the policy and procedures for its use that protect electronic PHI and control access to it.

2.22 "Unsecured PHI" or "PHI that is unsecured" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of Health and Human Services ("HHS") in the guidance issued on the HHS Web site.

2.23 "Use" shall have the meaning given to such term under the HIPAA regulations at 45 CFR §160.103.

3. OBLIGATIONS AND ACTIVITIES OF CONTRACTOR AS BUSINESS ASSOCIATE.

3.01 CONTRACTOR agrees not to use or further disclose PHI that CITY discloses to CONTRACTOR except as permitted or required by this Agreement or by law.

3.02 CONTRACTOR agrees to use appropriate safeguards, as provided for in this Agreement, to prevent use or disclosure of PHI that CITY discloses to CONTRACTOR or that CONTRACTOR creates, receives, maintains, or transmits, on behalf of CITY, except as provided for by this Contract.

3.03 CONTRACTOR agrees to comply with the HIPAA Security Rule, at Subpart C of 45 CFR Part 164, with respect to electronic PHI that CITY discloses to CONTRACTOR or that CONTRACTOR creates, receives, maintains, or transmits, on behalf of CITY.

3.04 CONTRACTOR agrees to mitigate, to the extent practicable, any harmful effect of a Use or Disclosure of PHI by CONTRACTOR in violation of the requirements of this Agreement that becomes known to CONTRACTOR.

3.05 CONTRACTOR agrees to immediately report to CITY any Use or Disclosure of PHI not provided for by this Agreement that CONTRACTOR becomes aware of. CONTRACTOR must report Breaches of Unsecured PHI in accordance with 45 CFR §164.410.

3.06 CONTRACTOR agrees to ensure that any of its subcontractors that create, receive, maintain, or transmit, PHI on behalf of CONTRACTOR agree to comply with the applicable requirements of Section 164 Part C by entering into a contract or other arrangement.

3.07 To comply with the requirements of 45 CFR §164.524, CONTRACTOR agrees to provide access to CITY, or to an individual as directed by CITY, to PHI in a Designated Record Set within fifteen (15) calendar days of receipt of a written request by CITY.

3.08 CONTRACTOR agrees to make amendment(s) to PHI in a Designated Record Set that CITY directs or agrees to, pursuant to 45 CFR §164.526, at the request of CITY or an Individual, within thirty (30) calendar days of receipt of the request by CITY. CONTRACTOR agrees to notify CITY in writing no later than ten (10) calendar days after the amendment is completed.

3.09 CONTRACTOR agrees to make internal practices, books, and records, including policies and procedures, relating to the use and disclosure of PHI received from, or created or received by CONTRACTOR on behalf of CITY, available to CITY and the Secretary in a time and manner as determined by CITY, or as designated by the Secretary, for purposes of the Secretary determining CITY'S compliance with the HIPAA Privacy Rule.

3.10 CONTRACTOR agrees to document any Disclosures of PHI that CITY discloses to CONTRACTOR or that CONTRACTOR creates, receives, maintains, or transmits on behalf of CITY, and to make information related to such Disclosures available as would be required for CITY to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR §164.528.

3.11 CONTRACTOR agrees to provide CITY information in a time and manner to be determined by CITY in order to permit CITY to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR §164.528.

3.12 CONTRACTOR agrees that, to the extent CONTRACTOR carries out CITY's obligation(s) under the HIPAA Privacy and/or Security rules, CONTRACTOR will comply with the requirements of 45 CFR Part 164 that apply to CITY in the performance of such obligation(s).

3.13 CONTRACTOR shall work with CITY upon notification by CONTRACTOR to CITY of a Breach to properly determine if any Breach exclusions exist as defined below.

4. SECURITY RULE.

4.01 CONTRACTOR shall comply with the requirements of 45 CFR § 164.306 and establish and maintain appropriate Administrative, Physical and Technical Safeguards in accordance with 45 CFR §164.308, §164.310, §164.312, §164.314 and §164.316 with respect to electronic PHI that CITY discloses to CONTRACTOR or that CONTRACTOR creates, receives, maintains, or transmits on behalf of CITY. CONTRACTOR shall follow generally accepted system security principles and the requirements of the HIPAA Security Rule pertaining to the security of electronic PHI.

4.02 CONTRACTOR shall ensure that any subcontractors that create, receive, maintain, or transmit electronic PHI on behalf of CONTRACTOR agree through a contract with CONTRACTOR to the same restrictions and requirements contained here.

4.03 CONTRACTOR shall immediately report to CITY any Security Incident of which it becomes aware. CONTRACTOR shall report Breaches of Unsecured PHI as described in 5. BREACH DISCOVERY AND NOTIFICATION below and as required by 45 CFR §164.410.

5. BREACH DISCOVERY AND NOTIFICATION.

5.01 Following the discovery of a Breach of Unsecured PHI, CONTRACTOR shall notify CITY of such Breach, however, both parties may agree to a delay in the notification if so advised by a law enforcement official pursuant to 45 CFR §164.412.

5.01.1 A Breach shall be treated as discovered by CONTRACTOR as of the first day on which such Breach is known to CONTRACTOR or, by exercising reasonable diligence, would have been known to CONTRACTOR.

5.01.2 CONTRACTOR shall be deemed to have knowledge of a Breach, if the Breach is known, or by exercising reasonable diligence would have been known, to any person who is an employee, officer, or other agent of CONTRACTOR, as determined by the federal common law of agency.

5.02 CONTRACTOR shall provide the notification of the Breach immediately to the CITY DEH Executive Director or other designee.

5.02.1 CONTRACTOR'S initial notification may be oral, but shall be followed by written notification within 24 hours of the oral notification.

5.03 CONTRACTOR'S notification shall include, to the extent possible:

5.03.l The identification of each Individual whose Unsecured PHI has been, or is reasonably believed by CONTRACTOR to have been, accessed, acquired, used, or disclosed during the Breach;

5.03.2 Any other information that CITY is required to include in the notification to each Individual under 45 CFR §164.404 (c) at the time CONTRACTOR is required to notify CITY, or

promptly thereafter as this information becomes available, even after the regulatory sixty (60) day period set forth in 45 CFR §164.410 (b) has elapsed, including:

1. A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;

2. A description of the types of Unsecured PHI that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

3. Any steps Individuals should take to protect themselves from potential harm resulting from the Breach;

4. A brief description of what CONTRACTOR is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any future Breaches; and

5. Contact procedures for Individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

5.04 CITY may require CONTRACTOR to provide notice to the Individual as required in 45 CFR §164.404, if at the sole discretion of the CITY, it is reasonable to do so under the circumstances.

5.05 In the event that CONTRACTOR is responsible for a Breach of Unsecured PHI in violation of the HIPAA Privacy Rule, CONTRACTOR shall have the burden of demonstrating that CONTRACTOR made all required notifications to CITY, and as required by the Breach notification regulations, or, in the alternative, that the acquisition, access, use, or disclosure of PHI did not constitute a Breach.

5.06 CONTRACTOR shall maintain documentation of all required notifications of a Breach or its risk assessment under 45 CFR §164.402 to demonstrate that a Breach did not occur.

5.07 CONTRACTOR shall provide to CITY all specific and pertinent information about the Breach, including the information listed above, if not yet provided, to permit CITY to meet its notification obligations under Subpart D of 45 CFR Part 164 as soon as practicable, but in no event later than fifteen (15) calendar days after CONTRACTOR's initial report of the Breach to CITY.

5.08 CONTRACTOR shall continue to provide all additional pertinent information about the Breach to CITY as it becomes available, in reporting increments of five (5) business days after the prior report to CITY. CONTRACTOR shall also respond in good faith to all reasonable requests for further information, or follow-up information, after report to CITY, when such request is made by CITY.

5.09 In addition to the provisions in the body of the Agreement, CONTRACTOR shall also bear all expense or other costs associated with the Breach and shall reimburse CITY for all expenses CITY incurs in addressing the Breach and consequences thereof, including costs of investigation, notification, remediation, documentation or other costs or expenses associated with addressing the Breach.

6. PERMITTED USES AND DISCLOSURES BY CONTRACTOR.

6.01 CONTRACTOR may use or further disclose PHI that CITY discloses to CONTRACTOR as necessary to perform functions, activities, or services for, or on behalf of, CITY as specified in the Agreement, provided that such use or Disclosure would not violate the HIPAA Privacy Rule if done by CITY.

6.02 CONTRACTOR may use PHI that CITY discloses to CONTRACTOR, if necessary, for the proper management and administration of the Agreement.

6.03 CONTRACTOR may disclose PHI that CITY discloses to CONTRACTOR to carry out the legal responsibilities of CONTRACTOR, if:

6.03.1 The Disclosure is required by law; or

6.03.2 CONTRACTOR obtains reasonable assurances from the person or entity to whom/which the PHI is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person or entity and the person or entity immediately notifies CONTRACTOR of any instance of which it is aware in which the confidentiality of the information has been breached.

6.04 CONTRACTOR may use or further disclose PHI that CITY discloses to CONTRACTOR to provide Data Aggregation services relating to the Health Care Operations of CONTRACTOR.

6.05 CONTRACTOR may use and disclose PHI that CITY discloses to CONTRACTOR consistent with the minimum necessary policies and procedures of CITY.

7. OBLIGATIONS OF CITY.

7.01 CITY shall notify CONTRACTOR of any limitation(s) in CITY'S notice of privacy practices in accordance with 45 CFR §164.520, to the extent that such limitation may affect CONTRACTOR'S Use or Disclosure of PHI.

7.02 CITY shall notify CONTRACTOR 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 CONTRACTOR'S Use or Disclosure of PHI.

7.03 CITY shall notify CONTRACTOR of any restriction to the Use or Disclosure of PHI that CITY has agreed to in accordance with 45 CFR §164.522, to the extent that such restriction may affect CONTRACTOR'S use or disclosure of PHI.

7.04 CITY shall not request CONTRACTOR to use or disclose PHI in any manner that would not be permissible under the HIPAA Privacy Rule if done by CITY.

8. BUSINESS ASSOCIATE TERMINATION.

8.01 Upon CITY'S knowledge of a material breach or violation by CONTRACTOR of the requirements of this Contract, CITY shall:

8.01.1 Provide an opportunity for CONTRACTOR to cure the material breach or end the violation within thirty (30) business days; or

8.01.2 Immediately terminate the Agreement, if CONTRACTOR is unwilling or unable to cure the material breach or end the violation within (30) days, provided termination of the Agreement is feasible.

8.02 Upon termination of the Agreement, CONTRACTOR shall either destroy or return to CITY all PHI CONTRACTOR received from CITY and any and all PHI that CONTRACTOR created, maintained, or received on behalf of CITY in conformity with the HIPAA Privacy Rule.

8.02.1 This provision shall apply to all PHI that is in the possession of subcontractors or agents of CONTRACTOR.

8.02.2 CONTRACTOR shall retain no copies of the PHI.

8.02.3 In the event that CONTRACTOR determines that returning or destroying the PHI is not feasible, CONTRACTOR shall provide to CITY notification of the conditions that make return or destruction infeasible. Upon determination by CITY that return or destruction of PHI is infeasible, CONTRACTOR shall extend the protections of this Agreement to the PHI and limit further Uses and Disclosures of the PHI to those purposes that make the return or destruction infeasible, for as long as CONTRACTOR maintains the PHI.

8.03 The obligations of this Agreement shall survive the termination of the Agreement.

9. <u>SUBSTANCE ABUSE (42 C.F.R., Part 2).</u>

CONTRACTOR shall also comply with all provisions of 42 C.F.R., Part 2 relating to substance abuse treatment and records.

EXHIBIT G, FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) – the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor – a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

_____ _____

Printed Name/Signature of Contractor Employee Date

_____ _____

Printed Name/Signature of Contractor Representative Date

_____

Organization and Title of Contractor Representative