REVISED
BID RESPONSE PACKET
710-25-049

BID SIGNATURE PAGE

Type or Print the following information.

PROSPECTIVE CONTRACTOR'S INFORMATION					
Company:	ModivCare Solutions, LLC				
Address:	6900 E. Layton Ave Suite 1200				
City:	Denver	State:	CO	Zip Code:	80237
Business Designation:	□ Individual □ Partnership	□ Sole Proprietorship ☒ Corporation	□ Public Service Corp □ Nonprofit		
Minority and Women-Owned Designation*:	☒ Not Applicable □ African American □ Asian American	□ American Indian □ Hispanic American □ Pacific Islander American	□ Service Disabled Veteran □ Women-Owned		
	AR Certification #: ________________	* See *Minority and Women-Owned Business Policy*			

PROSPECTIVE CONTRACTOR CONTACT INFORMATION *Provide contact information to be used for bid solicitation related matters.*			
Contact Person:	Marvin O. Lewis	Title:	VP of Contracts and Pricing
Phone:	404-888-5854	Alternate Phone:	800-486-7647
Email:	marvinl@modivcare.com		

CONFIRMATION OF REDACTED COPY

□ YES, a redacted copy of submission documents is enclosed.

□ NO, a redacted copy of submission documents is not enclosed. I understand a full copy of non-redacted submission documents will be released if requested.

Note: If a redacted copy of the submission documents is not provided with Prospective Contractor's response packet, and neither box is checked, a copy of the non-redacted documents, with the exception of financial data (other than pricing), will be released in response to any request made under the Arkansas Freedom of Information Act (FOIA). See Bid Solicitation for additional information.

COMBINDED CERTIFICATIONS FORM

Prospective Contractor has included, in this submission packet, the signed Attachment H-Combined Certifications for Contracting with the State of Arkansas.

An official authorized to bind the Prospective Contractor to a resultant contract must sign below.

The signature below signifies agreement that any exception that conflicts with a Requirement of this *Bid Solicitation* **will cause the Prospective Contractor's bid to be disqualified:**

Authorized Signature: Marvin O. Lewis **Title:** VP of Contracts and Pricing

Printed/Typed Name: Marvin O. Lewis **Date:** 06/26/2025

SECTIONS 1 - 4 VENDOR AGREEMENT AND COMPLIANCE

- *Any requested exceptions to items in this section which are NON-mandatory **must** be declared below or as an attachment to this page. Vendor **must** clearly explain the requested exception and should label the request to reference the specific solicitation item number to which the exception applies.*

- *Exceptions to Requirements **shall** cause the vendor's proposal to be disqualified.*

By signature below, vendor agrees to and **shall** fully comply with all requirements as shown in the bid solicitation.

Vendor Name:	ModivCare Solutions, LLC	**Date:**	06/26/2025
Signature:		**Title:**	VP of Contracts and Pricing
Printed Name:	Marvin O. Lewis		

PROPOSED SUBCONTRACTORS FORM

- ***Do not*** *include additional information relating to subcontractors on this form or as an attachment to this form.*

PROSPECTIVE CONTRACTOR PROPOSES TO USE THE FOLLOWING SUBCONTRACTOR(S) TO PROVIDE SERVICES.

Type or Print the following information

Subcontractor's Company Name	Street Address	City, State, ZIP
ALS Transportation LLC.	4305 S CARAWAY RD.	JONESBORO, AR 72404
Comply Services LLC.	1500 GEYER ST.	LITTLE ROCK, AR 72202
Ealy Transportation	293 SOLOMON GROVE RD.	TWIN GROVES, AR 72039
Helping Hand NMT LLC.	3840 GRIGGS AVE.	JONESBORO, AR 72401
LLACC Transportation	900 CARSON CV.	CONWAY, AR 72034
LYFT Healthcare Inc.	185 BERRY ST. STE 400	SAN FRANCISCO, CA 94107
Manuels Express Transport LLC.	510 PEA RIDGE ST.	CONWAY, AR 72032
Moses & Brenda Transport LLC.	806 MELODY LN.	BLYTHEVILLE, AR 72315
National Mobility Eldercare Inc. dba Envoy	17767 N. PERIMETER DR. STE B-109	SCOTTSDALE, AZ 85288
No Longer Bound Ministries	1104 W. PLEASURE AVE.	SEARCY, AR 72143
Oasis Facility Solutions LLC.	110 E. KIEHL AVE. STE 1A	SHERWOOD, AR 72120
Perry Boys Transportation LLC.	115 N. GUTHRIE ST.	SPIRO, OK 74959
ProMed Logistics LLC.	7 DANUBE DR	MAUMELLE, AR 72113
Star Express Transport LLC.	200 W. STILLWELL AVE	DE QUEEN, AR 74738
Treasured Transportation- AR	1025 S. PARKSIDE ST.	BLYTHEVILLE, AR 72315
UBER Health LLC.	1725 THRID ST.	SAN FRANCISCO, CA 94158
Uplift LLC. - AR	300 5th AVE. NE	GRAVETTE, AR 72736
WHC Little Rock dba zTrip	7510 JAMISON RD.	LITTLE ROCK, AR 72209
Walker Courier Transportation Services	9703 LANEHART RD.	LITTLE ROCK, AR 72204

☐ PROSPECTIVE CONTRACTOR DOES NOT PROPOSE TO USE SUBCONTRACTORS TO PERFORM SERVICES.

STATEMENT OF ATTESTATION

The Broker shall provide written assurance to DHS that all vehicles used for Beneficiary transport will be in compliance with all requirements of the Arkansas Transportation Department for Arkansas Intrastate Renewal prior to award and upon any contract renewal periods.

By signature below, the Prospective Contractor agrees to and shall fully comply with all requirements as described in this attestation.

Authorized Signature: Marvin O. Lewis

Printed Name: Marvin O. Lewis Date: 06/26/2025

DOCUMENTATION CHECKLIST

As outlined in section 2.2 Minimum Qualifications in the solicitation document, please provide the following:

- Letter of Bondability
- Active registration from the Arkansas Secretary of State’s Office, or other state approved documentation
- Official Bid Price Sheet
- All documents provided in the bid response packet
- Copy of Vendor’s Equal Opportunity Policy
- Signed Addenda, if applicable
- EO 98-04 Disclosure Form (Attachment A)
- Client History Form (Attachment I)
- Combined Certifications (Attachment H)
- Job descriptions for specific roles as outlined in §2.2.C of the solicitation document.
- Attachment J – ARDHS – OIT-Standard IT Requirements as outlined in Section 2.31 of the solicitation document

OFFICIAL BID PRICE SHEET

710-25-049 Non-Emergency Medical Transportation Services

All costs **must** be included in the unit price. Costs not included in the unit price below are not billable under a contract established from this solicitation. Bidder must submit a printed copy of the completed official bid price sheet with bid submission.

Instructions: Enter the per member per month unit price for each region being bid. DHS will not accept bids that do not fall within the actuarial spread range listed below.

ITEM	DESCRIPTION	Actuarial Spread	UNIT PRICE (per member per month)
1	Region A	$3.44-$3.56	$3.44
2	Region B	$7.85-$8.07	$7.85
3	Region C	$4.95-$5.15	$4.95
4	Region D	$5.71-$5.92	$5.92
5	Region E	$11.67-$12.08	$12.08
6	Region F	$16.59-$17.23	$16.59
7	Region G	$6.39-$6.53	$6.39

AUTHORIZED SIGNATURE:

By my signature below, I certify that the I am authorized by the respondent to submit this bid on his/her behalf.

Vendor Name: ModivCare Solutions, LLC　Date: 06/26/2025

Signature: Marvin O. Lewis　Title: VP of Contracts and Pricing

Printed Name: Marvin O. Lewis

modivcare

Arkansas Supplement

TABLE OF CONTENTS

PAGE

GENERAL INFORMATION

About This Arkansas Supplement

Modivcare is committed to workplace policies and practices that comply with federal, state and local laws. For this reason, Arkansas team members will receive the Company's Team Member handbook ("Team Member Handbook") and the Arkansas Supplement to the Team Member Handbook ("Arkansas Supplement") (together, the "Handbook").

The Arkansas Supplement applies only to Arkansas team members. It is intended as a resource containing specific provisions derived under Arkansas law that apply to the team member's employment. It should be read together with the Team Member Handbook and, to the extent that the policies in the Arkansas Supplement are different from, or more generous than those in the Team Member Handbook, the policies in the Arkansas Supplement will apply.

The Arkansas Supplement is not intended to create a contract of continued employment or alter the at-will employment relationship. **Only the Chief Executive Officer (CEO) of the Company or his or her authorized representative has the authority to enter into an agreement that alters the at-will employment relationship and any such agreement must be in writing signed by the Chief Executive Officer (CEO) of the Company or his or her authorized representative**.

If team members have any questions about these policies, they should contact their supervisor, Human Resources, or another member of management.

COMMITMENT TO DIVERSITY

Equal Employment Opportunity

As set forth in the employee handbook, Modivcare is committed to equal employment opportunity and compliance with federal antidiscrimination laws. We also comply with Arkansas law, which prohibits discrimination and harassment against team members or applicants for employment based on race, color, religion, gender, pregnancy or related medical condition, age (40 and over), national origin or ancestry, citizenship, sensory, mental or physical disability, genetic information and military service. The Company will not tolerate discrimination or harassment based upon these characteristics or any other characteristic protected by applicable federal, state or local law.

PAY PRACTICES

Lactation Accommodation

The Company provides accommodations to nursing team members and to team members with a need to express breast milk (also referred to as pumping, collectively referred to herein as “expressing breast milk”) during work hours. The Company will provide 20 minute paid pumping breaks, the frequency of which depends on the hours worked, each day to accommodate a team member desiring to express breast milk for the team member’s nursing child in accordance with state and local law requirements. If additional breaks are required, team members should work with their supervisor regarding scheduling.

The Company will provide team members with the use of a private location, other than a toilet stall, for the team member to express milk. Team members should discuss with their supervisor, any member of management, or Human Resources the location to express their breast milk and for storage of expressed milk and to make any other arrangements under this policy. The Company may not be able to provide additional break time or a private location for expressing breast milk, if doing so would substantially disrupt the Company’s operations.

Team members should provide reasonable notice to the Company that they intend to take breaks for expressing breast milk upon returning to work. The Company reserves the right not to provide such additional time if to do so would unduly burden operations.

The Company will not demote, terminate or otherwise take adverse action against an team member who requests or makes use of the accommodations and break time described in this policy.

TIME OFF & LEAVES OF ABSENCE

Military Leave

Arkansas team members who are called to active state duty as a member of the state’s armed forces, including the National Guard, a service component of the armed forces or the militia, are entitled to the same rights, privileges, benefits and protections as team members called to action to serve in the United States military. Team members called to active state duty in Arkansas are entitled to a leave of absence and reemployment rights in accordance with the Military Leave Policy set forth in the Team Member Handbook.

Team members will not be denied retention in employment because of the team member’s obligation as a member of the armed forces.

Jury Duty Leave

The Company encourages all team members to fulfill their civic responsibilities and to respond to a jury service summons or subpoena, attend court for prospective jury service or serve as a juror. Under no circumstances will team members be terminated, threatened, coerced or penalized because they respond to a jury service summons or subpoena, attend court for prospective jury service or serve as a juror.

Team members must provide their supervisor with notice of any jury summons or subpoena within a reasonable time after receipt and before their appearance is required. Verification from the court clerk of having served may also be required.

Time spent engaged in attending court for prospective jury service or for serving as a juror is not compensable except that exempt team members will not incur any reduction in pay for a partial week's absence due to jury duty. Team members who are absent from work for time spent responding to a summons and/or subpoena, for participating in the jury selection process, or for serving as a juror, will not be asked or required to use any annual, vacation or sick leave during the absence, although team members may be permitted to do so.

Time Off To Vote

The Company encourages team members to fulfill their civic responsibilities and to vote in all public elections. Most team members’ schedules provide sufficient time to vote either before or after working hours.

Any team member who does not have sufficient time to vote outside of working hours may be excused from work for a reasonable period of time, to vote. The time off will be without pay for nonexempt team members.

The Company asks that team members request time off to vote from their supervisor at least one day prior to Election Day so that the time off can be scheduled to minimize disruption to normal work schedules. Proof of having voted may be required.

Bone Marrow or Organ Donation Leave

Team members who undergo a medical procedure to donate bone marrow or an organ will be provided with Unpaid time off, not to exceed 90 days. Team members seeking leave under this policy must submit a written request to their supervisor and to your Human Resources Business Partner

Leave under this policy is not available to a team member who is eligible for leave under the Family and Medical Leave Act.

Crime Victim Leave

Eligible team members who are the victim or the representative of a victim of a crime or sex offense will be provided with time off to:

- Participate, at the prosecuting attorney's request, in the preparation of a criminal justice proceeding relating to the crime; or

- Attend a criminal justice proceeding if attendance is reasonably necessary to protect the interests of the victim.

Time off under this policy will be unpaid, except that exempt team members will be paid when required by applicable federal or state law. Team members are eligible for time off if they are:

- The victim of the sex offense or violent crime (felony resulting in physical injury to the victim or involving the use of a deadly weapon, terroristic threatening, and stalking) at issue in the proceedings;

- A minor who is a victim of kidnapping, false imprisonment, permanent detention or restraint;

- The victim's spouse, child by birth or adoption, stepchild, parent, stepparent or sibling; or

- An individual designated by the victim or by a court in which the crime is being, or could be prosecuted.

Team members who are accountable for the crime or a crime arising from the same conduct are not eligible for leave under this policy.

Before team members may take time off from work for this purpose, they must provide their supervisor with advance notice and, if possible, a copy of the notice of proceeding. Confidentiality of the situation, including the team member's request for the time off under this policy, will be maintained to the greatest extent possible.

The Company will not retaliate, nor tolerate retaliation, against any team member who seeks or obtains leave under this policy.

WORKPLACE SAFETY AND SECURITY

Smoke-Free Workplace

The Company prohibits smoking marijuana or any other substance that is illegal under federal law or Arkansas law anywhere on its premises.

The Company also prohibits smoking in the workplace. Team members wishing to smoke must do so outside company facilities during scheduled work breaks.

Team members that observe other individuals smoking in the workplace in violation of this policy have a right to object and should report the violation to their supervisor or another member of management. Team members will not be disciplined or retaliated against for reporting a smoking violation or otherwise exercising their rights under Arkansas law or this policy.

Team members that violate this policy may be subject to disciplinary action up to and including termination of employment.

Cell Phone Use/Texting While Driving

As set forth in the Team Member Handbook, cellular telephones are not to be used while driving. Team members should also be aware that using a wireless telecommunications device while driving to (1) write, send, or read a text-based communication, or (2) access, read, or post to a social networking site are violations of Arkansas law, in addition to being a violation of company policy. Drivers are, however, permitted to read, select, or enter a telephone number or name in a wireless telecommunications device for the purpose of making a telephone call.

It is also a violation of Arkansas law for a driver to use a handheld wireless telephone for any reason, other than in an emergency, when passing a school building or school zone during school hours when children are present and outside the building.

No Weapons in the Workplace

In the interest of maintaining a workplace that is safe and free of violence, and in accordance with the policy set forth in the employee handbook, the Company generally prohibits the presence or use of firearms and other weapons on the Company’s property, regardless of whether or not the person is licensed to carry the weapon.

However, in compliance with Arkansas law, the Company does not prohibit team members who lawfully possess firearms from transporting or storing their legally owned and lawfully possessed firearms inside their locked, privately-owned vehicles in the Company’s parking lots. The Company reserves the right to make certain limited exceptions to this policy in accordance with Arkansas law. The firearm may not be removed from the team members' personal vehicle or displayed to others.

Contract Number ______________

Attachment Number ______________

Action Number ______________

CONTRACT AND GRANT DISCLOSURE AND CERTIFICATION FORM

Failure to complete all of the following information may result in a delay in obtaining a contract, lease, purchase agreement, or grant award with any Arkansas State Agency.

SUBCONTRACTOR: □ **Yes** ☑**No**

SUBCONTRACTOR NAME: ModivCare Solutions, LLC

IS THIS FOR: **Goods?** □ **Services?** ☑ **Both?** □

TAXPAYER ID NAME: ModivCare Solutions, LLC

YOUR LAST NAME: Lewis **FIRST NAME** Marvin **M.I.:** O

ADDRESS: 6900 E.Layton Ave. Suite 1200

CITY: Denver **STATE:** CO **ZIP CODE:** 80237 **COUNTRY:** US

AS A CONDITION OF OBTAINING, EXTENDING, AMENDING, OR RENEWING A CONTRACT, LEASE, PURCHASE AGREEMENT, OR GRANT AWARD WITH ANY ARKANSAS STATE AGENCY, THE FOLLOWING INFORMATION MUST BE DISCLOSED:

FOR INDIVIDUALS*

Indicate below if: you, your spouse or the brother, sister, parent, or child of you or your spouse *is* a current or former: member of the General Assembly, Constitutional Officer, State Board or Commission Member, or State Employee:

Position Held	Mark (√)		Name of Position of Job Held [senator, representative, name of board/ commission, data entry, etc.]	For How Long?		What is the person(s) name and how are they related to you? [i.e., Jane Q. Public, spouse, John Q. Public, Jr., child, etc.]	
	Current	Former		From MM/YY	To MM/YY	Person's Name(s)	Relation
General Assembly							
Constitutional Officer							
State Board or Commission Member							
State Employee							

XX□ **None of the abopp a lies**

FOR AN ENTITY (BUSINESS)*

Indicate below if any of the following persons, current or former, hold any position of control or hold any ownership interest of 10% or greater in the entity: member of the General Assembly, Constitutional Officer, State Board or Commission Member, State Employee, or the spouse, brother, sister, parent, or child of a member of the General Assembly, Constitutional Officer, State Board or Commission Member, or State Employee. Position of control means the power to direct the purchasing policies or influence the management of the entity.

Position Held	Mark (√)		Name of Position of Job Held [senator, representative, name of board/commission, data entry, etc.]	For How Long?		What is the person(s) name and what is his/her % of ownership interest and/or what is his/her position of control?		
	Current	Former		From MM/YY	To MM/YY	Person's Name(s)	Ownership Interest (%)	Position of Control
General Assembly								
Constitutional Officer								
State Board or Commission Member								
State Employee								

XX□ **None of the above applies**

Contract Number ____________
Attachment Number ____________
Action Number ____________

Contract and Grant Disclosure and Certification Form

Failure to make any disclosure required by Governor's Executive Order 98-04, or any violation of any rule, regulation, or policy adopted pursuant to that Order, shall be a material breach of the terms of this contract. Any contractor, whether an individual or entity, who fails to make the required disclosure or who violates any rule, regulation, or policy shall be subject to all legal remedies available to the agency.

As an additional condition of obtaining, extending, amending, or renewing a contract with a *state agency* I agree as follows:

1. Prior to entering into any agreement with any subcontractor, prior or subsequent to the contract date, I will require the subcontractor to complete a **Contract and Grant Disclosure and Certification Form**. Subcontractor shall mean any person or entity with whom I enter an agreement whereby I assign or otherwise delegate to the person or entity, for consideration, all, or any part, of the performance required of me under the terms of my contract with the state agency.

2. I will include the following language as a part of any agreement with a subcontractor:

   Failure to make any disclosure required by Governor's Executive Order 98-04, or any violation of any rule, regulation, or policy adopted pursuant to that Order, shall be a material breach of the terms of this subcontract. The party who fails to make the required disclosure or who violates any rule, regulation, or policy shall be subject to all legal remedies available to the contractor.

3. No later than ten (10) days after entering into any agreement with a subcontractor, whether prior or subsequent to the contract date, I will mail a copy of the **Contract and Grant Disclosure and Certification Form** completed by the subcontractor and a statement containing the dollar amount of the subcontract to the state agency.

I certify under penalty of perjury, to the best of my knowledge and belief, all of the above information is true and correct and that I agree to the subcontractor disclosure conditions stated herein.

Signature Marvin O. Lewis Title V.P. of Contracts and Pricing Date 07/14/2025

Vendor Contact Person Marvin O. Lewis Title V.P. of Contracts and Pricing Phone No. 800-486-7647

Agency use only

Agency Number 0710 Agency Name Department of Human Services Agency Contact Person ____________ Contact Phone No. ____________ Contract or Grant No. ____________

Department of Transformation and Shared Services
Governor Sarah Huckabee Sanders
Secretary Leslie Fisken

COMBINED CERTIFICATIONS FOR CONTRACTING WITH THE STATE OF ARKANSAS

Pursuant to Arkansas law, a vendor must certify as specified below and as designated by the applicable laws.

1. **Israel Boycott Restriction:** For contracts valued at $1,000 or greater.
   A public entity shall not contract with a person or company (the "Contractor") unless the Contractor certifies in writing that the Contractor is not currently engaged in a boycott of Israel. If at any time after signing this certification the Contractor decides to boycott Israel, the Contractor must notify the contracting public entity in writing. *See* Arkansas Code Annotated § 25-1-503.

2. **Illegal Immigrant Restriction:** For contracts valued at $25,000 or greater.
   No state agency may contract for services with a Contractor who knowingly employs or contracts with an illegal immigrant. The Contractor shall certify that it does not knowingly employ, or contract with, illegal immigrants. *See* Arkansas Code Annotated § 19-11-105.

3. **Energy, Fossil Fuel, Firearms, and Ammunition Industries Boycott Restriction:** For contracts valued at $75,000 or greater.
   A public entity shall not contract unless the contract includes a written certification that the Contractor is not currently engaged in and agrees not to engage in, a boycott of an Energy, Fossil Fuel, Firearms, or Ammunition Industry for the duration of the contract. *See* Arkansas Code Annotated § 25-1-1102.

4. **Scrutinized Company Restriction:** Required with bid or proposal submission.
   A state agency shall not contract with a Scrutinized Company or a company that employs a Scrutinized Company as a subcontractor. A Scrutinized Company is a company owned in whole or with a majority ownership by the government of the People's Republic of China. A state agency shall require a company that submits a bid or proposal for a contract to certify that it is not a Scrutinized Company and does not employ a Scrutinized Company as a subcontractor. *See* Arkansas Code Annotated § 25-1-1203.

By signing this form, the Contractor agrees and certifies they are not a Scrutinized Company and they do not currently and shall not for the aggregate term of any resultant contract:

- Boycott Israel.
- Knowingly employ or contract with illegal immigrants.
- Boycott Energy, Fossil Fuel, Firearms, or Ammunition Industries.
- Employ a Scrutinized Company as a subcontractor.

Contract Number: ____________________ Description: ____

Agency Name: ____

Vendor Number: __________________ Vendor Name: ModivCare Solutions, LLC

06/26/2025

Vendor Signature

Date

Attachment I
Client History Form
NON-EMERGENCY MEDICAL TRANSPORTATION SERVICES
710-25-049

Attachment I

Non-Emergency Medical Transportation Services

Instructions: This form is intended to help the State gain a more complete understanding of each Respondent's experience. This form **must** be completed completely and accurately.

The State reserves the right to verify the accuracy of these answers by contacting any of the listed clients, and all applicable clients **must** be listed. Omission of a client will constitute a failure to complete this form.

For purposes of this form, the "client" is not an individual but the entity which held the contract. By way of explanation, in the Contract resulting from this IFB, Arkansas DHS will be the client. For each listed client, Respondents may (but are not required) provide the contact information for a person at the client entity who is knowledgeable of the named project. If the State contacts clients listed on this form, the State reserves the right to contact the listed individual or another person at the listed client.

The boxes below each prompt will expand if necessary. The form **must** be signed (please see the final page) by the same signatory who signed the Response Signature Page.

1. Provide a narrative detailing your five (5) years of qualifying experience where you (the prime contractor only) served as the prime contractor for providing non-emergency transportation as a broker. Subcontractor experience shall not substitute for Broker experience. For each client, please specify the organization/agency/division, not just the state or political subdivision. Please briefly describe the scope of the contract and duration of services. If there are no contracts which meet this definition, please state "none."

Please see added supplement to this Client History Form

2. Please list job descriptions of staff proposed to fill the following required positions. A single staff member shall not serve in more than two (2) of these designated roles:

Project Director	Please see added supplement to this Client History Form
Safety Officer	Please see added supplement to this Client History Form
Quality Assurance Manager	Please see added supplement to this Client History Form
Investigator	Please see added supplement to this Client History Form
Trainer	Please see added supplement to this Client History Form

Authorized Signature: Marvin O. Lewis **Title:** VP of Contracts and Pricing V.P. of Contracts and Pricing

Printed/Typed Name: Marvin O. Lewis Marvin O. Lewis **Date:** 06/26/2025 06/30/2025

Attachment I Client History Form

1. Provide a narrative detailing your five (5) years of qualifying experience where you (the prime contractor only) served as the prime contractor for providing non-emergency transportation as a broker. Subcontractor experience shall not substitute for Broker experience. For each client, please specify the organization/agency/division, not just the state or political subdivision. Please briefly describe the scope of the contract and duration of services. If there are no contracts which meet this definition, please state "none."

Modivcare NEMT Experience

Since 1997, Modivcare has been a leading provider of full-service non-emergency medical transportation (NEMT) brokerage programs for Medicaid and Medicare entities nationwide. As the first broker to implement a statewide NEMT brokerage model, we pioneered the framework that continues to influence industry standards to this day. With over two decades of proven innovation and operational excellence, we currently serve as the NEMT broker of choice for 14 state Medicaid agencies and more than 103 managed care organizations, overseeing 121 transportation programs across all 50 states and the District of Columbia.

The four engagements outlined below highlight our relevant experience within the past five years. Each example reflects our direct oversight of large-scale NEMT programs—either statewide or regionally—including all core functions such as provider network management, member services, trip scheduling, claims processing, regulatory compliance, and performance monitoring.

1. Oklahoma Health Care Authority (OHCA) – SoonerRide Program

Agency: Oklahoma Health Care Authority (OHCA)
Scope: Statewide NEMT brokerage
Duration: 2003 – Present (22+ years; including all five most recent years)

Modivcare has served as the sole NEMT broker for Oklahoma's SoonerRide program since 2003. In this role, we provide comprehensive NEMT services for over 325,000 Medicaid members per month. Our scope includes all aspects of program delivery—eligibility verification, reservations, scheduling, provider network management, claims processing, and customer service. Our in-depth understanding of Oklahoma's healthcare access challenges, especially in rural and frontier regions, has enabled us to build a trusted, locally rooted transportation network. We maintain strategic partnerships with 16 Rural Public Transit (5311) providers who deliver 32% of all NEMT trips in the state. Additionally, our long-term partnership with OHCA reflects sustained high performance, innovation (e.g., Comdata mileage reimbursement cards), and substantial cost savings for the state.

2. West Virginia Department of Health and Human Resources (WV DHHR)

Agency: West Virginia Bureau for Medical Services
Scope: Statewide NEMT brokerage
Duration: 2018 – Present (7 years)

Modivcare began serving as the statewide NEMT broker for West Virginia in 2018. We successfully transitioned from the state's previous vendor and established full operations under an aggressive implementation timeline. The contract scope includes full-service NEMT brokerage for over 600,000 covered lives, with more than 2.1 million annual trips and 718,000+ calls managed each year. We support the Bureau's goals through an integrated model leveraging public transit, mileage reimbursement, and behavioral health facility-based transport. Our implementation success was recognized by the West Virginia Governor's Office with a proclamation declaring "Modivcare Day" in 2018.

3. Maine Department of Health and Human Services (DHHS), Office of MaineCare Services (OMS)

Agency: Maine DHHS, OMS
Scope: Regional NEMT brokerage across five of Maine's eight regions
Duration: 2013 – Present (12+ years; all five recent years included)

Initially awarded Region 8 in 2013, Modivcare expanded to Regions 1, 2, 6, and 7 in 2014. We now serve a combined Medicaid population of approximately 145,000 members, managing over 2.2 million annual trips and 277,000+ annual calls. The contract scope includes program design, implementation, and operations management for each region. Our solution resolved major performance issues from a previous vendor and rapidly restored trust in the state's NEMT program. Innovations include public transit partnerships, expanded network capacity, and vehicle acquisitions to support same-day and urgent trips. Within seven months of expansion, we achieved a 95.8% satisfaction rating from MaineCare members.

4. Georgia Department of Community Health (DCH)

Agency: Georgia Department of Community Health
Scope: Statewide NEMT brokerage
Duration: 1997 – Present (28+ years; all five recent years included)

Modivcare has served as Georgia's statewide NEMT broker since 1997. Over the past five years, we have managed transportation for hundreds of thousands of Medicaid members, with full responsibility for reservations, provider dispatch, call center operations, compliance, and technology integration. We maintain a 24/7/365 Georgia-based call center and have implemented a robust Business Continuity and Disaster Recovery (BC/DR) plan that has been activated successfully in response to numerous emergencies, including hurricanes, winter storms, and the COVID-19 pandemic. Our performance has consistently met DCH's standards, and our contract has been renewed multiple times over two decades.

2. Please list job descriptions of staff proposed to fill the following required positions. A single staff member shall not serve in more than two (2) of these designated roles:

Project Director

POSITION SUMMARY

The Project Director reports to the General Manager and is responsible for coordinating with the GM to ensure the success of local/statewide contract(s). Responsibilities include establishing and maintaining excellent relationships with clients and providers, meeting performance standards, and achieving financial goals.

ESSENTIAL FUNCTIONS

- Monitoring transportation company performance

- Enforcing contract standards; and managing transportation costs and rate issues.

- Requires strong financial/ analytical skills for data and cost analysis; strong organizational independence and prioritization capability; ability to communicate effectively with clients and providers and make public presentations.

- Must be technically capable of developing programs and an organizational structure to support contract requirements.

- Must be able to conceptualize process flow both in establishing policies and in enhancing our proprietary computer-aided system.

- Must be project-oriented and hands-on from planning to delivery of outcome, to include the ability to identify issues and implement resolutions.

- Qualified candidates will possess a proven track record of success in people development and management, impeccable written communication skills, and a high level of technical competence, including Microsoft Office suite - Excel, Word, Access, and Outlook. Must be able to work independently and as a team member.

POSITION QUALIFICATIONS

Competency Statement(s)
Analytical Skills - Strong ability to use thinking and reasoning to solve a problem.
Communication, Oral - Excellent ability to communicate effectively with others using the spoken word.

Communication, Written - Excellent ability to communicate in writing, clearly and concisely.

Customer Oriented - Excellent ability to take care of the customers' needs while following company procedures.

Decision Making - Ability to make critical decisions while following company procedures.

Interpersonal - Ability to get along well with a variety of personalities and individuals.

Leadership - Ability to influence others to perform their jobs effectively and to be responsible for making decisions.

Proficient in the use of Word, Excel, Outlook, and PowerPoint. Excellent oral and written communication skills, Management Skills - Excellent ability to organize and direct oneself and effectively supervise others.

Problem Solving - Excellent ability to find a solution for or to deal proactively with work-related problems.

Relationship Building - Ability to effectively build relationships with customers and co-workers.

Working Under Pressure - Driven ability to complete assigned tasks under stressful situations.

EDUCATION & EXPERIENCE

Education

- BA/BS in Business, Management, Finance, or relevant field required; Graduate Degree preferred

- 8 years of progressive management experience in transportation, call center, distribution, logistics, and/or health care

Experience

- Must have experience managing multiple direct reports

- Must have prior experience developing and managing budgets; researching variances

- Transportation or Call Center Industry experience a plus • Demand-response transportation management experience a pl

SKILLS

- Strong financial/analytical skills

- Excellent written and verbal communication skills

- Proven track record of success in people management

- Strong leadership skills; excellent organization and planning skills

- Able to manage effectively at all levels

- High energy, self-motivated, analytical, with excellent communication and problem-solving skills

- Excellent Presentation Skills • Must be solutions-oriented, creative, innovative thinker

- Must be able to develop and implement action plans to address issues

- Must be able to analyze state and regional data and costs

- Must feel comfortable and sound substantive in public speaking engagements

- Must be able to discuss issues with local government officials

- Expert proficiency with Microsoft Excel, Outlook, and Word; intermediate proficiency with Microsoft Access a plus

WORK ENVIRONMENT

The work environment characteristics described here are representative of those an employee encounters while performing the essential functions of this job.

- Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

- Entire work time is conducted in an office environment in a controlled atmosphere building.

- The noise level in the work environment is usually moderate.

COMPLIANCE ESSENTIAL FUNCTIONS

- Adhere to all federal, state, and other relevant policies, procedures, regulations, and guidelines applicable to this role

- Complete Compliance training upon hire and annually thereafter

- Immediately report any suspected fraud, waste or abuse, conflicts of interest, or other potential compliance incidents to Modivcare's Chief Compliance Officer

Officer or Legal Department

- Demonstrate a high standard of ethics while assisting leadership in upholding Modivcare's culture of compliance (supervisors and above

SAFETY OFFICER

POSITION SUMMARY

This position is responsible for overseeing and implementing safety programs and initiatives within a specific region. The role ensures compliance with local, state, and federal safety regulations and develops strategies to minimize workplace accidents and injuries. The Safety Manager conducts regular inspections and audits, identifies potential hazards, and provides training and education to teammates on safety protocols. This role collaborates with management and staff to create a culture of safety and implement best practices. Additionally, the role investigates incidents and accidents, maintains safety records, and develops emergency response plans.

ESSENTIAL JOB FUNCTIONS AND RESPONSIBILITIES

- Facilitates and coordinates the implementation of safety policies and procedures in compliance with local, state, and contractual regulations.

- Conducts regular safety inspections and audits to identify hazards and ensure compliance with OSHA and other regulatory standards.

- Develops, delivers, and administers effective company-wide safety training programs and materials, including those related to the Integrated Business Planning (IBP) plan.

- Serves as a technical advisor and facilitator of training and safety in support of each region, providing guidance and support to employees and management on safety-related issues.

- Investigates accidents, incidents, and near misses to determine root causes, recommend corrective actions, and lead the implementation of standardized investigative practices.

- Develops and maintains strong relationships with company leaders, clients, and government agencies through regular communication of safety programs and progress.

- Collaborates with management and Risk Management staff to develop and implement safety policies and procedures that align with organizational goals.

- Maintains accurate records of safety inspections, incidents, training, and other relevant activities, and prepare monthly reports on injury and risk metrics, training status, audits, and regulatory compliance issues.

- Monitors and analyzes safety performance metrics to identify trends and areas for improvement, staying current with industry trends, regulations, and best practices.

- Liaises with regulatory bodies and external auditors during inspections and audits, ensuring preparedness and compliance.

- Sets goals, plan timetables, and maintain control of processes and reporting functions to ensure goals are met and safety standards are raised.

- Reports weekly to the Safety Director.

- Participates in other projects or duties as assigned.

- Occasional business travel is required.

SUPERVISORY RESPONSIBILITIES

- N/A

KNOWLEDGE, SKILLS AND ABILITIES

- Strong knowledge of OSHA regulations and other relevant safety standards.

- Strong training and teaching skills, with the ability to effectively educate and engage employees on safety protocols and best practices.

- Excellent analytical and problem-solving skills.

- Effective communication and presentation skills.

- Ability to develop and implement comprehensive safety training programs.

- Proficiency in conducting safety audits and risk assessments.

- Strong organizational and record-keeping abilities.

- Ability to work independently and manage multiple priorities.

- Strong interpersonal skills with the ability to collaborate across various levels of the organization.

- Proficiency in using safety management software and Microsoft Office Suite.

EDUCATION AND TRAINING

- Bachelor's Degree in Occupational Health and Safety, Environmental Science, or a related field required.

- Five (5) plus years of experience.

- Community Transportation Association of America Master certification required, or must be actively working towards obtaining it.

- Or equivalent combination of education and/or experience.

Other Competencies

- Drive for Results - Establishes aggressive goals and takes appropriate, calculated risks to achieve results. Acts with a sense of urgency regarding personal and organizational goals and priorities. Demonstrates discipline and does the right thing, even when it is difficult. Shows determination and persistence in the face of challenges.

- Customer-Focused - Listens to understand the customer’s perspective and is patient with their frustrations and struggles. Anticipates customer needs and demonstrates commitment to exceeding their expectations. Shares ideas on how to enhance the customer experience. Builds rapport with customers through being empathetic and demonstrating reliability.

- Self-Awareness - Thinks through possible outcomes and impact on others before taking action. Recognizes strong emotional reactions and directs the energy into productive behavior and communication. Can articulate personal values and aspirations. Leverages personal strengths while working on managing weaknesses.

- Valuing Others - Values and embraces the individuality of others by treating everyone with dignity, respect, and compassion. Appreciates other cultures and perspectives and seeks common ground through listening and demonstrating empathy. Credits others for their contributions and accomplishments. Builds relationships across the organization through transparency and extending trust to others.

- Learning Agility and Development - Seeks out and takes on challenging assignments to broaden skills and perspective. Proactively seeks out resources to support personal development (books, articles, online resources, company resources, subject matter experts, etc.) Reflects on and discusses successes and failures to learn and strive for continuous improvement. Continuously seeks feedback from peers and leaders on growth opportunities.

- Innovation - Seeks and shares ideas to improve work processes, from small tweaks to large changes. Applies the creative ideas from others and embraces opportunities to pilot and experiment. Reflects on and discusses how new ideas and processes impact other teams and the customer. Adjusts to changing conditions and finds ways to get the work done

Core Values

- We treat everyone with dignity and RESPECT

- We earn the TRUST of our members, and each other

- We provide RELIABLE services that open doors

- We serve with courtesy and COMPASSION

- We prioritize SAFETY

- We communicate with purpose and TRANSPARENCY

COMMENTS:

The above statements are intended to describe the general nature and level of work being performed by individuals in this position. Other functions may be assigned, and management retains the right

to add or
change the duties at any time.

QUALITY ASSURANCE MANAGER

POSITION SUMMARY

The Quality Assurance (QA) Manager executes the QA Plan, which includes Complaint/Concern management, Notice Of Action investigation/ resolution, and special projects as needed. The QA Supervisor also has oversight of the activities of the Quality Assurance Department and establishes positive and effective working relationships with customers, providers, and agencies to establish superior customer service and to reduce the number of official complaints. Identifies the highest complaint categories and devises action plans and monitors complaints for immediate and effective reduction of those categories.

ESSENTIAL FUNCTIONS

- Identify the highest complaint categories and devise action plans

- Monitors complaints for immediate and effective reduction of the highest complaint categories

- Supervises all Quality Assurance (QA) Representatives and Field Monitors

- Assists all QA Representatives with overflow complaints when necessary and with tasks and problem-solving

- Prepares and sends certified letters to customers

- Tags and identifies recorded conversations and monitors phone conversations between representatives and clients

- Handles and processes customer complaints when unresolved at the representative level

- Attends supervisory staff meeting

- Implements instructions and policies throughout the department, resolves staff concern,s and serves as a liaison to other departments

- Closes out all customer complaints in Excel

- Works closely with Transportation Coordinators, scheduling reservations and dispatching

- Processes and resolves both in-house and client complaints

- Retrieves trip and provider information from LCAD system

• Logs all complaints and faxes all complaints to the appropriate provider for response within three business days

• Copies all complaints in the transmittal log and files all complaints in the appropriate provider book

• Maintains individualized jurisdictional logs and enters information by date received and date due

POSITION QUALIFICATIONS

Competency Statement(s)

- Analytical Skills - Strong ability to use thinking and reasoning to solve a problem.
- Communication, Oral - Excellent ability to communicate effectively with others using the spoken word.
- Communication, Written - Excellent ability to communicate in writing, clearly and concisely.
- Customer Oriented - Excellent ability to take care of the customers' needs while following company procedures.
- Decision Making - Ability to make critical decisions while following company procedures.
- Interpersonal - Ability to get along well with a variety of personalities and individuals.
- Leadership - Ability to influence others to perform their jobs effectively and to be responsible for making decisions.
- Proficient in the use of Word, Excel, Outlook, and PowerPoint. Excellent oral and written communication skills. Management Skills - Excellent ability to organize and direct oneself and effectively supervise others.
- Problem Solving - Excellent ability to find a solution for or to deal proactively with work-related problems.
- Relationship Building - Ability to effectively build relationships with customers and co-workers.
- Working Under Pressure - Driven ability to complete assigned tasks under stressful situations.

EDUCATION & EXPERIENCE

• AA or BA/BS required

Experience
• 5+ years relevant work experience
• Demonstrated experience interacting with individuals, families, mental health, elder services, and health care facilities and programs.
• Exceptional interpersonal, written, and verbal skills.
• Knowledge of clinical UR and QA, Medicaid, Medicare guidelines, and covered services.
• Supervisory experience required to include demonstrated people management skills and motivation techniques.

SKILLS

- Strong attention to detail and thoroughness
- Computer proficiency with Microsoft Office, Excel, and Access.

WORK ENVIRONMENT

The work environment characteristics described here are representative of those an employee encounters while performing the essential functions of this job.

- Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.
- Entire work time is conducted in an office environment in a controlled atmosphere building.
- The noise level in the work environment is usually moderate

INVESTIGATOR

This position is responsible for conducting thorough investigations into allegations of fraud, misconduct, and other irregularities. Additionally, this role will involve in gathering and analyzing evidence, interviewing witnesses and suspects, and preparing detailed reports on your findings.

ESSENTIAL JOB FUNCTIONS AND RESPONSIBILITIES

- Analyzes data trends and creates reports to identify suspicious activity and recommend corrective actions.

- Collaborates with law enforcement, regulatory agencies, legal professionals, and internal departments to support investigations and fraud mitigation efforts.

- Develops and implements investigative strategies, ensuring adherence to industry standards and legal requirements.

- Maintains detailed case documentation, prepares investigative reports, and testifies in hearings or legal proceedings as needed.

- Provides training and guidance to internal teams on fraud detection and prevention techniques.

- Conducts detailed interviews, investigates potential occurrences of FWA, gathers necessary evidence, documents findings, and procedures utilized during the investigations.

- Applies analytical skills to case reviews and assessments.

- Performs interviews and documents findings to appropriate internal and external stakeholders.

- Advises management team on issues relating to FWA investigations processes.

- Processes faxes, mail, email, and web requests (inbound and outbound) related to allegations or
patterns indicating potential or actual FWA.

- Reports to management team bona fide allegations of potential or actual FWA.

- Leads regular & ad hoc status calls with clients or law enforcement regarding allegations or patterns indicating potential or actual FWA .

- Partners with Network Services personnel to fulfill internal, client, or law enforcement requests for
field investigations involving allegations or patterns indicating potential or actual FWA.

- Provides outreach and education to members, facilities, clients, law enforcement, and company
personnel regarding FWA, as needed.

- Leverages internal and external resources, including communications with members, facilities, clients, law enforcement, and other parties, to fully investigate potential or actual FWA.

- May lead projects and perform other duties as assigned.

- Occasional business travel may be required.

SUPERVISORY RESPONSIBILITIES

- N/A

KNOWLEDGE, SKILLS AND ABILITIES

- Excellent customer service and people skills.
- Must be able to work independently and with teams.
- Ability to quickly learn new technology and processes.
- Must be able to understand and follow complex instructions.
- Read, write, speak, and understand English fluently.

EDUCATION AND TRAINING

- High School Diploma or GED required.
- Two (2) plus years of experience in law enforcement, military, or SIU.
- Or equivalent combination of education and/or experience.

OTHER COMPETENCIES

• Drive for Results - Establishes aggressive goals and takes appropriate, calculated risks to achieve results. Acts with a sense of urgency regarding personal and organizational goals and priorities. Demonstrates discipline and does the right thing, even when it is difficult. Shows determination and persistence in the face of challenges.

• Customer-Focused - Listens to understand the customer’s perspective and is patient with their frustrations and struggles. Anticipates customer needs and demonstrates commitment to exceeding their expectations. Shares ideas on how to enhance the customer experience. Builds rapport with customers through being empathetic and demonstrating reliability.

• Self-Awareness - Thinks through possible outcomes and impact on others before taking action.
Recognizes strong emotional reactions and directs the energy into productive behavior and communication. Can articulate personal values and aspirations. Leverages personal strengths while working on managing weaknesses.

• Valuing Others - Values and embraces the individuality of others by treating everyone with dignity, respect, and compassion. Appreciates other cultures and perspectives and seeks common ground through listening and demonstrating empathy. Credits others for their contributions and accomplishments. Builds relationships across the organization through transparency and extending trust to others.

• Learning Agility and Development - Seeks out and takes on challenging assignments to broaden skills and perspective. Proactively seeks out resources to support personal development
(books, articles, online resources, company resources, subject matter experts, etc.) Reflects on and continuously seeks feedback from peers and leaders on growth opportunities.

• Innovation - Seeks and shares ideas to improve work processes, from small tweaks to large changes. Applies the creative ideas from others and embraces opportunities to pilot and experiment. Reflects on and discusses how new ideas and processes impact other teams and the
customer. Adjusts to changing conditions and finds ways to get the work done

CORE VALUES

• We treat everyone with dignity and RESPECT

• We earn the TRUST of our members, and each other

• We provide RELIABLE services that open doors

• We serve with courtesy and COMPASSION

• We prioritize SAFETY

• We communicate with purpose and TRANSPARENCY

COMMENTS:

The above statements are intended to describe the general nature and level of work being performed by
individuals in this position. Other functions may be assigned, and management retains the right to add or
change the duties at any time.

Trainer

POSITION SUMMARY

The Trainer provides all business units with necessary training to ensure proficiency in the daily operation of the business. The Trainer offers ongoing coaching and provides assistance to management as necessary by monitoring the performance of CSRs and conducting new hire training and refresher courses. The Trainer develops and updates all training manuals, handouts, and training aids using client guidelines.

ESSENTIAL FUNCTIONS

- Assist Call Center Supervisor and Manager in overseeing functions of the CSRs
- Ensure a high level of customer serviceand promotes a positive workingenvironment
- Establish and maintaingood working relationship with providers, clients,co-workers, and regional office personnel
- Assist Call Centermanagement with completing agent reports and report statistics to Call Center management
- Provide Call
  Centermanagement with feedbackfor 90 days and annualevaluations of CSRs
- Comply with Modivcare’s policies and procedures
- Assist clients with any transportation concerns
- Assist in the identification of system problemsand reports any malfunctioning equipment to Call Center management
- Attend all required meetings
- Maintain an acceptable attendance and tardinessrecord based on company attendance policy
- Develop and update all training manuals, handouts and training aids for call center and regional offices
- Ensure customer service/ call taking is standardized statewide through on- site training initiatives

- Ensure call centernew hire paperwork and files are completed in a timelyfashion and distributed to appropriate departments and/or supervisor
- Conduct new hire training for call center employees
- Perform call monitoring and productivity measurement; provides feedback to managers
- Use quality monitoring database to compile,track and trendindividual and team (regional) performance
- Provide feedback for training alongwith providing coaching/ training to employees as needed to improve performance

POSITION QUALIFICATIONS

Competency Statement(s)

- Accurate - Abilityto perform work accurately and thoroughly
- Communication,Oral - Ability to communicate effectively with othersusing the spoken word
- Communication,Written - Abilityto communicate in writing clearlyand concisely
- Customer Oriented - Ability to take care of the customers’ needswhile following company procedures
- Interpersonal- Ability to get along well with a varietyof personalities and individuals
- Patience - Abilityto act calmly under stressand strain, and of not being hastyor impetuou s
- Reliability - Dependable and trustworthy
- Ability to thinkcreatively and use various methodsin problem solving;ability to anticipate and resolve problems
- Ability to teach,coach, motivate and lead new hires and frontline staff
- Positive attitude and ability to work well with others

Education

- High School Graduateor General EducationDegree (GED)

Experience

- Two to Five (2-5) years heavy phone volume customerservice experience to include inboundcall center/customer service experience
- One (1)+ years demonstrated experience coaching and training call center staff preferred.

Skills

- Excellent customer serviceand phone skills
- Superior communication and problem-solvingskills
- Must be able to work independently and as a part of a team
- Ability to fosterand maintain a positive environment
- Ability to quicklylearn new technology
- Must be able to understand and follow complexinstructions

- Ability to accurately type 35 wpm
- Read and writeEnglish fluently
- Proficient in Microsoft Word, Excel, and Outlook
- Bilingual a plus
- Proficient with MicrosoftWord, Excel, and Outlook
- Must be able tohandle heavy phonevolume

Physical Demands

The physical demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this Job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

While performing the duties of this Job, the employeeis regularly requiredto talk or hear. The employee is frequently required to use hands to finger, handle, or feel. The employee is occasionally required to stand, walk, reach with hands and arms. Specific vision abilities required by this Job include close vision.

Work Environment

The work environment characteristics described here are representative of those an employee encounters while performing the essential functionsof this Job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

- Entire work time is conducted in an officeenvironment in a controlled atmosphere building.
- The noise levelin the work environment is usually moderate.
- This job specification should not be construed to imply that these requirements are the exclusive standards of the position. Incumbents will followany other instructions and perform other related duties as may be required by their supervisor.

Arkansas Secretary of State
Cole Jester

State Capitol Building ♦ Little Rock, Arkansas 72201-1094 ♦ 501-682-3409

Certificate of Good Standing

I, Cole Jester, Secretary of State of the State of Arkansas, and as such, keeper of the records of domestic and foreign corporations, do hereby certify that the records of this office show

MODIVCARE SOLUTIONS, LLC

formed under the laws of the state of Delaware, and authorized to transact business in the State of Arkansas as a Foreign Limited Liability Company, was granted a Registration of Foreign Limited Liability Company by this office May 24, 2006.

Our records reflect that said entity, having complied with all statutory requirements in the State of Arkansas, is qualified to transact business in this State.

In Testimony Whereof, I have hereunto set my hand and affixed my official Seal. Done at my office in the City of Little Rock, this 10th day of June 2025.

Cole Jester
Secretary of State

Online Certificate Authorization Code: e34ebdd64a65fdb
To verify the Authorization Code, visit sos.arkansas.gov

State of Arkansas
DEPARTMENT OF HUMAN SERVICES
700 South Main Street
P.O. Box 1437 / Slot W345
Little Rock, AR 72203

ADDENDUM 1

TO: All Addressed Vendors
FROM: Office of Procurement
DATE: June 6, 2025
SUBJECT: 710-25-049 Non-Emergency Medical Transportation Services

The following change(s) to the above referenced IFB have been made as designated below:

______ Change of specification(s)
______ Additional specification(s)
______ Change of bid opening date and time
______ Cancellation of bid
__X__ Other

OTHER

- Attachment D – remove and replace with Attachment D Revised Terms and Conditions.

The specifications by virtue of this addendum become a permanent addition to the above referenced IFB. Failure to return this signed addendum may result in rejection of your proposal.

If you have any questions, please contact: Ian Cunningham, DHS.OP.Solicitations@dhs.arkansas.gov; (501) 682-0120.

06/25/2025

Vendor Signature　　　　Date

ModivCare Solutions, LLC

Company

State of Arkansas
DEPARTMENT OF HUMAN SERVICES
700 South Main Street
P.O. Box 1437 / Slot W345
Little Rock, AR 72203

ADDENDUM 2

TO: All Addressed Vendors
FROM: Office of Procurement
DATE: June 24, 2024
SUBJECT: 710-25-049 Non-Emergency Medical Transportation Services

The following change(s) to the above referenced IFB have been made as designated below:

______ Change of specification(s)
______ Additional specification(s)
______ Change of bid opening date and time
______ Cancellation of bid
__X__ Other

OTHER

- Add Written Questions and Answers
- Bidders Library
    - Add the following: 710-25-049 Exhibit 3
    - Add the following: 710-25-049 Exhibit 4
- Solicitation – remove and replace with 710-25-049 Solicitation Revision 1 (Redline and Clean versions)
- Attachment C – remove and replace with Revised Attachment C (Redline and Clean versions)
- Response Packet – remove and replace with Revised 710-25-049 Response Packet
- Additional Questions and Answers period

Deadline for Receipt of Written Questions	June 26, 2025
Response to Written Questions, On or About	June 30, 2025

The specifications by virtue of this addendum become a permanent addition to the above referenced IFB. Failure to return this signed addendum may result in rejection of your proposal.

If you have any questions, please contact: Ian Cunningham
DHS.OP.Solicitations@dhs.arkansas.gov
(501) 682-0120

06/25/2025

Vendor Signature

Date

ModivCare Solutions, LLC

Company

State of Arkansas
DEPARTMENT OF HUMAN SERVICES
700 South Main Street
P.O. Box 1437 / Slot W345
Little Rock, AR 72203

ADDENDUM 3

TO: All Addressed Vendors
FROM: Office of Procurement
DATE: June 30, 2025
SUBJECT: 710-25-049 Non-Emergency Medical Transportation Services

The following change(s) to the above referenced IFB have been made as designated below:

__X__ Change of specification(s)
_____ Additional specification(s)
__X__ Change of bid opening date and time
_____ Cancellation of bid
__X__ Other

CHANGE OF SPECIFICATIONS

- Section 2.31.E — Remove and replace with:

  E. The Broker **must** comply with DHS/Office of Information Technology (OIT) Standard information technology requirements, as specified in Attachment J – ARDHS – OIT-Standard IT Requirements.

  1. For verification purposes, the Prospective Contractor **shall** include the completed Attachment J: ARDHS OIT Standard IT Requirements within fourteen (14) days of contract award. If a Prospective Contractor responds with "Does Not Apply" to a requirement in Attachment J, the Prospective Contractor **shall** add an explanation in the Comments column. DHS will review the submission and incorporate the submission and any updates required by DHS to the Contractor in the resulting contract.

- Solicitation – remove and replace with 710-25-049 Solicitation Revision 2 (Redline and Clean versions)

CHANGE OF BID OPENING DATE AND TIME

- Bid Submission date and time has been extended to July 7, 2025, 10:00 a.m. CST
- Bid Opening date and time has been extended to July 7, 2025, 11:00 a.m. CST

OTHER

- 710-25-049 Written Question and Answers — Remove and replace with 710-25-049 Revised Written Questions and Answers

The specifications by virtue of this addendum become a permanent addition to the above referenced IFB. Failure to return this signed addendum may result in rejection of your proposal.

If you have any questions, please contact:

Ian Cunningham
DHS.OP.Solicitations@dhs.arkansas.gov
(501) 682-0120

Vendor Signature

07/01/2025
Date

ModivCare Solutions, LLC
Company

Requirement Number	Requirement Group	Requirement Subgroup	Requirement	Comments	Meets Requirements	Describe How Requirements Met
1	Application Hosting	Batch – Job Control and Scheduling	Any technology vendor, application or solution shall develop, document and manage the processes and procedures for Interfaces and Batch Operations Architecture.		Yes	Modivcare maintains documented processes for managing all interfaces and batch operations architecture. These processes include specifications for data formats (e.g., JSON, XML, flat files), secure transfer protocols (HTTPS, SFTP), validation, logging, and error handling. Batch jobs and integrations are governed by formal change control, scheduling, and monitoring procedures. All interfaces and batch workflows are reviewed, approved, and version-controlled under Modivcare's system development lifecycle and change advisory processes. These procedures align with Modivcare's compliance frameworks, including HIPAA, SOC 2 Type II, HITRUST r2, and ISO 27001.
2	Application Hosting	Batch – Job Control and Scheduling	Any technology vendor, application or solution shall define job scheduling requirements, application software interdependencies, and rerun requirements for all production jobs		Yes	Modivcare defines job scheduling requirements and production job dependencies during system design and implementation. Each batch job includes documented scheduling parameters, upstream and downstream application interdependencies, and rerun conditions. These details are captured in operational runbooks and managed through Modivcare's change control process. If a job fails, automated alerts are triggered, and rerun procedures ensure data integrity and continuity. All job logic and dependencies are reviewed during deployment and monitored during operations.
3	Application Hosting	Batch – Job Control and Scheduling	Any technology vendor, application or solution shall utilize and manage scheduling tools for automating job execution (e.g., job workflow processes interdependencies, rerun requirements, file exchange functions, and print management)		Yes	Modivcare utilizes automated job scheduling tools to manage and execute production workflows, including batch processing, data file exchanges, and interdependent job execution. Scheduling tools are configured to define job workflows, set interdependencies, and enforce rerun logic based on predefined error-handling rules. Automated file transfers (e.g., via SFTP) are integrated into the schedule to support inbound and outbound data exchanges. Print management and other output functions are included as scheduled tasks where applicable. Job monitoring and alerting are built into the scheduling framework, enabling proactive error detection and recovery. All scheduling configurations are documented and maintained under Modivcare's change management process and reviewed as part of operational readiness and ongoing system support.
4	Application Hosting	Batch – Job Control and Scheduling	Any technology vendor, application or solution shall maintain a master job schedule and execute all batch jobs for the DHS Enterprise Program (e.g. any jobs provided by any vendor working on/with the DHS Enterprise Platform)		Yes	Modivcare maintains a master job schedule for all batch operations that interact with client systems, including coordination with external partners or platforms, such as the DHS Enterprise Program. The master job schedule includes execution timing, job dependencies, data inputs/outputs, and rerun procedures. This schedule is centrally managed and version-controlled to ensure consistency across environments and integration points. Modivcare collaborates with participating vendors to align scheduling dependencies and timing, ensuring that batch jobs are executed in accordance with shared requirements. Any jobs provided by or dependent on other vendors are integrated into the broader execution plan and tracked as part of the overall operational schedule. Updates to the job schedule follow a formal change control process and are reviewed for potential impacts before deployment. Monitoring tools are used to track job status, with alerts for failures or delays.
5	Application Hosting	Batch – Job Control and Scheduling	Any technology vendor, application or solution shall perform job monitoring and manage resolution of any failed jobs.		Yes	Modivcare performs active job monitoring for all scheduled and automated processes, including batch jobs, data exchanges, and file transfers. Monitoring tools are configured to detect job failures, delays, or abnormal runtime conditions. When a failure occurs, automated alerts are triggered and sent to the appropriate support teams for triage. Failed jobs are logged and tracked through Modivcare's incident and operations management processes. Root cause analysis is performed as needed, and rerun procedures are executed according to documented recovery steps to ensure data consistency. All resolution activities are recorded, and high-severity issues are escalated through formal incident response procedures, in alignment with Modivcare's SOC 2, HIPAA, and ISO 27001 compliance frameworks.
6	Application Hosting	Change/Release Management	Any technology vendor, application or solution shall adhere to the Information Technology Infrastructure Library (ITIL) V3.0 Change and Release Management processes.		Yes	Modivcare maintains a formal Change and Release Management process that aligns with the principles of ITIL v3.0, including structured change classification, approval, and deployment workflows. All production changes are tracked and reviewed based on risk level and potential business impact. High-risk or major changes are reviewed by a Change Advisory Board (CAB) and require documented testing, rollback planning, and formal approvals. Release deployments follow a defined schedule with stakeholder communication, and post-change validation and reviews are conducted as appropriate. These practices are enforced through Modivcare's internal ITSM processes and are audited under its SOC 2 Type II, ISO 27001, and HIPAA compliance programs.
7	Application Hosting	Change/Release Management	Any technology vendor, application or solution shall identify and submit any changes in compliance with the DHS Enterprise Program Change/Release Management process.		Yes	Modivcare will work with DHS to understand and align with the DHS Enterprise Program Change and Release Management process. Modivcare's existing internal change control procedures are structured around industry standards and can accommodate external change submission, documentation, and coordination workflows. Upon contract award, Modivcare will review DHS-specific change and release management requirements and integrate them into our operational process where applicable. Any necessary adjustments will be addressed through Modivcare's governance and compliance frameworks to ensure proper alignment, while maintaining internal controls consistent with SOC 2 Type II, ISO 27001, and HIPAA requirements.
8	Application Hosting	Disaster Recovery	Any technology vendor, application or solution shall maintain a detailed Disaster Recovery plan to meet Disaster Recovery requirements. Plan shall include plans for data, back-ups, storage management, and contingency operations that provides for recovering the DHS Enterprise Platform within established recovery requirement timeframes after a disaster that has affected the users of the DHS Enterprise Platform.		Yes	Modivcare maintains a documented Disaster Recovery Plan (DRP) that defines procedures for restoring critical systems, services, and data in the event of a disaster. The plan includes: - Data and Backup Procedures: Backups are performed regularly, encrypted, and stored in a secure, geographically separate location from production systems. Backup integrity is monitored and verified. - Storage and Retention Management: Data storage follows documented retention schedules, with controls in place to support redundancy and recoverability. - Contingency Operations: The DRP includes structured recovery workflows for applications, infrastructure, file systems, and access services. Periodic testing validates plan effectiveness and team readiness. Modivcare's DRP is developed and maintained under its SOC 2 Type II, ISO 27001, and HIPAA compliance frameworks. Upon contract award, Modivcare will review DHS-specific disaster recovery expectations—including any defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)—and ensure proper alignment through contractual agreements such as the MSA or BAA, as applicable.
9	Application Hosting	Disaster Recovery	Any technology vendor, application or solution shall provide support to the DHS support teams with implementing, configuring and testing disaster recovery.		Yes	Modivcare will support DHS support teams in the implementation, configuration, and testing of disaster recovery procedures for systems and services under Modivcare's responsibility. This includes: - Providing recovery documentation and technical input for DHS-integrated systems - Participating in disaster recovery exercises, including pre-test preparation, execution support, and post-test review - Assisting with configuration alignment and contingency planning to meet DHS expectations Modivcare's Disaster Recovery practices are developed and maintained in alignment with its certified compliance frameworks, including SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701. Upon contract award, Modivcare will work with DHS to define joint testing requirements, schedules, and communication protocols to ensure full integration with the DHS Enterprise Program's DR strategy.

10	Application Hosting	Disaster Recovery	Any technology vendor, application or solution shall develop action plans to address any issues arising from Disaster Recovery testing.		Yes	Modivcare conducts post-exercise reviews following disaster recovery (DR) tests to evaluate results, identify issues, and determine whether remediation is needed. Any issues uncovered during DR testing are assessed and tracked through Modivcare's incident management and change control processes. Depending on the nature of the issue, Modivcare assigns ownership, documents the resolution steps, and incorporates any necessary updates to recovery procedures or system configurations. These follow-up actions are recorded and reviewed as part of Modivcare's broader compliance and operational governance processes. This approach is consistent with Modivcare's control frameworks under SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701.
11	Application Hosting	Infrastructure Security	Any technology vendor, application or solution using cloud technology shall be located within the continental US. All servers and data will be located in US Soil.		Yes	Modivcare utilizes Amazon Web Services (AWS) for its primary cloud infrastructure, with hosting and data residency located exclusively in the U.S. East region. All production systems, backups, and data associated with Modivcare's services are hosted on servers physically located within the continental United States. Modivcare does not use offshore cloud services or store any client data outside U.S. borders. This ensures that all systems, data, and supporting infrastructure remain on U.S. soil, fully aligned with applicable security, privacy, and regulatory requirements. Cloud hosting is managed under Modivcare's compliance with HIPAA, SOC 2 Type II, HITRUST r2, ISO 27001, and ISO 27701.
12	Application Hosting	Infrastructure Security	Any technology vendor, application or solution shall proactively monitor all infrastructure including but not limited to network, storage, virtual environments, servers, databases, firewalls, etc. following industry best practices.		Yes	Modivcare proactively monitors its infrastructure, including network components, firewalls, virtual environments, servers, storage systems, and databases, using industry-standard monitoring tools and alerting frameworks. Monitoring is continuous and includes: - Real-time health and performance checks across all infrastructure layers - Threshold-based alerting for availability, latency, capacity, and security-related anomalies - Automated log collection and correlation for identifying potential incidents or degradation - Integration with incident response processes for prompt resolution and escalation Monitoring coverage extends to both cloud-hosted and on-premises systems, and all monitoring activities are aligned with NIST, ISO 27001, and SOC 2 Type II industry best practices. These processes are also subject to regular review under Modivcare's HIPAA and HITRUST r2 compliance programs.
13	Application Hosting	Infrastructure Security	Any technology vendor, application or solution shall implement physical and logical security within new functionality defined in the security plan consistent with DHS' security policies and industry standards.		Yes	Modivcare implements both physical and logical security controls for all systems and newly developed functionality in accordance with its enterprise security policies, which are aligned with industry standards and regulatory frameworks. Logical security includes role-based access controls (RBAC), multi-factor authentication, encryption, and secure system configurations. Physical security measures include restricted facility access, monitoring systems, and visitor logging at operational sites and data centers. Modivcare's secure development and change management processes incorporate security planning and validation prior to deployment. Following contract execution, Modivcare will review DHS-specific security requirements, including any referenced security plan, and will work to align new functionality accordingly through its established governance and compliance processes. Implementation of any DHS-specific controls or attestations will be subject to risk review, scoping, and internal planning timelines. These activities are governed by Modivcare's certified programs under SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701.
14	Application Hosting	Infrastructure Security	Any technology vendor, application or solution shall review all available infrastructure security patches relevant to the environment and classify the need and speed in which the security patches should be installed as defined by DHS security policies.		Yes	Modivcare maintains a formal vulnerability and patch management program that includes continuous review of vendor-issued and third-party security patches for infrastructure components such as servers, operating systems, databases, firewalls, and virtual environments. Security patches are assessed, prioritized, and applied based on severity, system criticality, and operational risk, using industry-standard classifications (e.g., CVSS scores, vendor threat bulletins). Patch urgency and implementation timing are defined through Modivcare's internal risk-based patch classification process, which supports emergency, high, and standard patching timelines. This process is governed under Modivcare's SOC 2 Type II, ISO 27001, and HITRUST r2 compliance frameworks. Following contract execution, Modivcare will review and consider DHS-specific security patching policies and classification standards. Alignment will be incorporated into Modivcare's patch management and change control procedures, subject to internal risk evaluation, planning, and operational timelines.
15	Application Hosting	Network, Hosting and Data Center Services	Any technology vendor, application or solution shall provision new environments and capacity as required to ensure performance requirements are met as volume increases and additional functionality is implemented.		Yes	Modivcare provisions new environments and scales system capacity as needed to support increases in transaction volume, user activity, and functionality. Modivcare's infrastructure is hosted in a scalable cloud environment (AWS), allowing for elastic resource provisioning based on workload demand. Capacity planning is integrated into Modivcare's architecture and operational monitoring processes. As usage thresholds are approached or new features are introduced, infrastructure teams evaluate resource needs and deploy additional compute, storage, or database instances as required. Performance baselines and thresholds are monitored in real time to support proactive scaling. New environments for development, testing, and production are provisioned in alignment with Modivcare's internal SDLC and change control policies. Upon contract award, Modivcare will assess any DHS-specific performance expectations or growth projections and incorporate them into capacity planning and infrastructure management efforts as appropriate. These practices are governed by Modivcare's compliance with SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701.
16	Application Hosting	Operating System, Application and Database Backup and Recovery	Any technology vendor, application or solution shall encrypt all data at rest including backups using DHS and regulatory bodies (CMS, FNS, etc.) standards regardless of storage media.		Yes	Modivcare provides data backup and restoration services in accordance with industry best practices. All production systems are backed up on a defined schedule using encrypted and automated backup processes, with storage in secure, logically separated environments. Key elements of Modivcare's backup and restoration practices include: - Encryption of all backup data at rest using strong, industry-standard algorithms - Geographic separation of backup storage from production systems - Automated monitoring and validation of backup integrity - Documented restoration procedures with predefined roles and audit logging Modivcare regularly reviews and tests its backup and restoration procedures to ensure recoverability. These processes are governed by certified frameworks including SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701. If additional DHS-specific backup requirements are defined, Modivcare will review and align with them following contract execution, subject to internal risk review and implementation planning.

17	Application Hosting	Storage Management Services	Any technology vendor, application or solution will provide data backup and restoration services in accordance with industry best practices.		Yes	Modivcare provides data backup and restoration services in accordance with industry best practices. All production systems are subject to automated backup processes, with backups stored in secure, access-controlled environments that are logically and geographically separate from primary production systems. Backup and restoration procedures include: Encryption of backup data at rest, using industry-standard cryptographic methods Defined backup schedules based on system criticality and recovery needs Regular integrity checks and automated monitoring of backup status Documented restoration procedures, including role assignments, escalation paths, and audit logging Modivcare tests its backup and restoration procedures periodically to validate recovery capabilities. These activities are governed by its certified compliance frameworks, including SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701. If DHS-specific backup standards or recovery expectations are defined, Modivcare will review and align with those requirements following contract execution, subject to internal review and implementation planning.
18	Application Hosting	Storage Management Services	Any technology vendor, application or solution will recommend techniques and procedures to ensure disk storage resources are utilized in an efficient and cost-effective manner.		Yes	Modivcare monitors and manages disk storage resources to support efficient and cost-effective utilization across its infrastructure. Storage is provisioned and scaled based on system usage patterns, data retention requirements, and application-specific performance needs. Modivcare applies the following techniques to optimize storage: - Tiered storage management to balance performance and cost - Monitoring and alerting for storage utilization thresholds and growth trends - Data lifecycle policies to manage archival, retention, and cleanup schedules - Compression and deduplication strategies where supported by the platform - Automated provisioning and right-sizing of cloud-based storage resources (e.g., in AWS) Storage usage is reviewed regularly by Modivcare's infrastructure and DevOps teams and adjusted as needed based on performance, capacity, and cost considerations. These practices are integrated into Modivcare's operational and compliance programs under SOC 2 Type II, ISO 27001, and HITRUST r2. Modivcare will review any DHS-specific storage requirements and provide additional recommendations as needed following contract execution.
19	Application Hosting	Storage Management Services	Any technology vendor, application or solution shall regularly test recovery procedures and practices to demonstrate recoverability and verify that actual practices are in concert with procedures and report results, as well as meet business requirements		Yes	Modivcare conducts regular testing of its recovery procedures and practices to validate the recoverability of systems and data and to confirm that operational execution aligns with documented recovery plans. These tests are designed to: - Demonstrate recoverability of critical systems, infrastructure, and data - Verify that recovery practices match documented procedures - Identify gaps or deviations, which are addressed through follow-up actions - Meet business continuity and contractual requirements Recovery tests are conducted periodically and may include full or partial failover scenarios, restoration of backup data, infrastructure recovery exercises, and tabletop simulations. Results are reviewed by Modivcare's IT, compliance, and operational leadership teams. Findings are documented and used to improve disaster recovery documentation and readiness posture. These testing practices are required and audited under Modivcare's certified frameworks, including SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701. If additional DHS-specific testing protocols or reporting formats are required, Modivcare will review and incorporate those requirements following contract execution, subject to internal planning and change control procedures.
20	Application Hosting	Storage Management Services	Any technology vendor, application or solution shall monitor and demonstrate compliance with Arkansas Records Retention Schedule.		Yes	Modivcare maintains documented data retention and destruction policies that align with applicable regulatory, contractual, and operational requirements. These policies govern how data is stored, archived, retained, and securely disposed of across systems that may handle state or client-owned data. Modivcare will review the Arkansas Records Retention Schedule and, upon contract execution, will work with DHS to align applicable record types, retention periods, and disposition procedures with Modivcare's internal compliance framework. Modivcare will incorporate these requirements into its data governance program through formal documentation, system configuration, and compliance monitoring, as appropriate. Retention and disposition activities are subject to Modivcare's control frameworks under HIPAA, HITRUST r2, SOC 2 Type II, ISO 27001, and ISO 27701, and are reviewed periodically for compliance with client-specific requirements.
21	Application Hosting	System Monitoring	Any technology vendor, application or solution shall manage and maintain monitoring procedures and standards for system/solution/infrastructure including, but not limited to: a. Monitoring of buffers, database buffers, table space fragmentation, database space, for unusual growth and propose a solution in case of alert b. Monitoring of system logs, update error, database corruption, jobs execution failures etc. and propose solution in case of an alert c. Monitoring of alert notification interface (e.g., Simple Mail Transfer Protocol (SMTP), sendmail), and propose a solution in case of an alert d. Monitoring of transaction and trace logs, network event logs and traces, garbage collector, memory and CPU utilization, indexes, etc., and propose a solution in case of an alert e. Monitoring of middleware (e.g., workflows, in- and out-bound queues) and report to DHS according to agreed procedure f. Monitoring and reporting of end-to-end transaction response time to allow measurements against SLAs g. Monitoring of interfaces h. Monitoring of batch jobs and job scheduling		Yes	Modivcare maintains and manages a comprehensive monitoring framework across its infrastructure, applications, databases, and integrations to ensure system health, performance, and SLA alignment. Monitoring is conducted in real time with automated alerting, logging, and escalation procedures. These monitoring standards are enforced through tools and practices that support Modivcare's certifications under SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701. Upon contract execution, Modivcare will review and align any DHS-specific alerting thresholds, escalation procedures, and reporting expectations into its monitoring framework.
22	Application Hosting	System Monitoring	Any technology vendor, application or solution shall monitor infrastructure for availability as well as transaction and response time performance.		Yes	Modivcare actively monitors its infrastructure for availability, transaction health, and end-to-end response time performance using industry-standard tools and automated alerting systems. Monitoring includes: - Infrastructure availability monitoring, covering servers, network components, virtual machines, storage systems, and hosted services - Transaction monitoring, including application-level performance, database query response times, and integration flows (e.g., APIs, batch jobs) - Response time telemetry, measured against internal performance baselines and service level objectives to detect latency or degradation trends When thresholds are exceeded or anomalies are detected, alerts are automatically generated and escalated to the appropriate operational teams for investigation and resolution. Performance metrics and uptime are reviewed regularly to support SLA compliance and capacity planning. These monitoring processes are governed under Modivcare's certified frameworks, including SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701. Modivcare will incorporate any additional DHS-specific availability or performance thresholds following contract execution, subject to internal review and integration planning.

23	Application Hosting	System Monitoring	Any technology vendor, application or solution shall provide regular monitoring reports of infrastructure performance, utilization and efficiency (e.g., proactive system monitoring)		Yes	Modivcare performs proactive monitoring of infrastructure and generates reports that reflect performance, utilization, and operational efficiency across systems and services. These reports are used internally by infrastructure and operations teams to support: - Capacity planning and resource optimization - Trend analysis for performance and availability - Identification of bottlenecks or abnormal usage patterns - Preventative actions to reduce system degradation or downtime Monitoring covers compute, memory, storage, network traffic, and transaction performance. Data from these systems is aggregated and visualized in dashboards or reports that are reviewed at regular intervals. Modivcare's reporting practices are governed by its internal IT operations framework and compliance requirements under SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701. If DHS-specific reporting content, formats, or frequencies are required, Modivcare will review and integrate those expectations following contract execution, subject to internal planning and reporting capabilities.
24	Application M&O Services	Disaster Recovery	Any technology vendor, application or solution shall identify and make available appropriate resources to support DHS' disaster recovery planning, testing and execution.		Yes	Modivcare will identify and make available appropriate technical and operational resources to support DHS disaster recovery (DR) planning, testing, and execution, as it relates to systems or services under Modivcare's responsibility. Modivcare assigns personnel with relevant expertise in infrastructure, data recovery, systems administration, and compliance to participate in DR planning and test coordination. Support may include: - Contributing to joint planning sessions and readiness assessments - Preparing and validating Modivcare-owned recovery procedures - Participating in DHS-led or joint DR test exercises - Providing post-test documentation or issue resolution, as applicable These activities are supported by Modivcare's certified governance under SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701. Specific staffing, timelines, and deliverables will be defined following contract execution in coordination with DHS and subject to internal planning and resource availability.
25	Application M&O Services	Security Administration	Any technology vendor, application or solution shall provide documented procedures for security monitoring and log management functions, and use write-once technology or other secure approaches for storing audit trails and security logs.		Yes	Modivcare maintains documented procedures for security monitoring and log management as part of its enterprise security and compliance program. These procedures govern the collection, analysis, retention, and protection of logs from infrastructure, applications, network components, and security systems. - Security logs and audit trails are: - Collected and centrally aggregated through monitoring tools - Reviewed regularly for anomalies, alerts, and indicators of compromise - Retained in accordance with internal policy and regulatory requirements - Protected from unauthorized access through role-based controls and restricted privileges - Stored using secure mechanisms that support immutability or integrity validation, such as access-controlled storage with append-only settings or cryptographic integrity checks While Modivcare does not currently assert use of "write-once" (WORM) storage across all environments, equivalent security controls are in place to ensure that audit trails and security logs cannot be modified or deleted once written, meeting the intent of immutability. These practices are reviewed under Modivcare's compliance with SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701. Upon contract execution, Modivcare will review any DHS-specific log storage or retention requirements and incorporate them into its log management framework, subject to internal evaluation and planning.
26	Data Governance	Master Data Management	Any technology vendor, application or solution shall provide data dictionary, data models, data flow models, process models and other related planning and design documents to DHS.		Yes	Modivcare maintains detailed planning and design documentation to support the development, integration, and operation of its technology solutions. Upon request and subject to the scope of services provided to DHS, Modivcare will provide relevant artifacts including: - Data dictionaries defining field-level metadata and business meaning - Data models representing schema structures, relationships, and constraints - Data flow diagrams and process models describing system interactions, inputs, outputs, and functional workflows - Additional design documentation, as appropriate, to support DHS review, integration, or system understanding All documentation is developed and version-controlled under Modivcare's Software Development Life Cycle (SDLC) and product operating model. Following contract execution, Modivcare will work with DHS to identify required documentation and delivery expectations, subject to data sensitivity, proprietary considerations, and confidentiality protections. These practices align with Modivcare's compliance obligations under SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701.
27	General System Behavior	Audit_&_Compliance	Any technology vendor, application or solution shall maintain a record (e.g. audit trail) of all additions, changes and deletions made to data in the applicable system or solution. In addition, a log of query or view access to certain type of records and/or screens will be maintained for investigative purposes. This should be readily searchable by user ID or client ID. This must include, but is not limited to: a. The user ID of the person who made the change b. The date and time of the change c. The physical, software/hardware and network location (IP address) of the person while making the change d. The information that was changed e. The outcome of the event f. The data before and after it was changed, and which screens were accessed and used		Yes	Modivcare maintains audit trails and access logs for all additions, changes, deletions, and views of sensitive data. Logged events are searchable by user ID, client ID, and timestamp, and are retained according to internal policy. Standard log elements include: - User ID of the person performing the action - Date and time of the event - IP address or network origin - Type of data accessed or changed - Outcome of the event (e.g., success/failure) - Before-and-after values, where applicable - Screen-level access activity, where system capabilities allow Logs are stored in secure, access-controlled environments and protected against tampering. These practices are reviewed under Modivcare's compliance with SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701. Upon contract execution, Modivcare will review DHS-specific audit logging requirements and align as appropriate, subject to system capabilities and internal governance.
28	General System Behavior	Audit_&_Compliance	Any technology vendor, application or solution shall prevent modifications to the audit records.		Yes	Modivcare implements controls to prevent unauthorized modification or deletion of audit records. Audit logs are stored in secure, access-controlled environments with role-based access restrictions to ensure that only authorized personnel can view but not alter log data. Additional protections include: - Write-restricted storage locations or append-only configurations - Separation of duties to prevent administrators from modifying logs - Monitoring of log access to detect and alert on any unauthorized activity These protections are reviewed regularly as part of Modivcare's compliance with SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701. Where applicable, integrity checks or cryptographic protections are used to further ensure log tamper resistance.

29	General System Behavior	Audit_&_Compliance	Any technology vendor, application or solution must have the ability to capture electronic signatures on all documents, forms, letters, and correspondences.		Yes	Modivcare supports the use of electronic signatures on documents, forms, letters, and correspondences, where applicable. Signature functionality is provided through integration with secure, standards-based e-signature platforms designed to meet regulatory requirements for authentication, traceability, and data protection. Capabilities include: - User authentication prior to signing - Timestamping and audit trail capture - Signature integrity validation and tamper detection - Storage of signed artifacts in secure, access-controlled systems Following contract execution, Modivcare will review DHS-specific document types, e-signature formats, and workflow requirements to confirm alignment within Modivcare's secure communications framework. These capabilities are maintained under Modivcare's certified compliance programs, including HIPAA, SOC 2 Type II, HITRUST r2, ISO 27001, and ISO 27701.
30	General System Behavior	Audit_&_Compliance	Any technology vendor, application or solution shall be able to detect security-relevant events (as defined in NIST 800-53 moderate baseline, rev 4) that it mediates and generate audit records for them. At a minimum the events will include, but not be limited to: a. Start/stop b. User login/logout c. Session timeout d. Account lockout e. Client record created/viewed/updated/deleted f. Scheduling g. Query h. Order i. Node-authentication failure j. Signature created/validated k. Personally Identifiable Information (PII) export l. PII import m. Security administration events n. Backup and restore o. Audit Event Types listed in IRS 1075		Yes	Modivcare detects and logs security-relevant events in accordance with industry standards and mapped controls from the NIST 800-53 rev. 4 moderate baseline. System and application logs capture key activity types, including: - System start/stop, login/logout, session timeout, and account lockout - Client data actions (create/view/update/delete), scheduling, queries, orders - Node-authentication failures and signature events - PII import/export and security administration activity - Backup, restore, and other system-level operations Audit logs include user ID, timestamp, source IP, event type, and outcome. Logs are securely stored, access-controlled, and protected from tampering. Logging procedures are reviewed under Modivcare's certified frameworks: SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701. Modivcare will review and align with DHS and IRS 1075 audit requirements following contract execution, subject to internal governance and system capability.
31	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution interfaces will secure and protect (encrypt) the data and the associated infrastructure from a confidentiality, integrity and availability perspective.		Yes	Modivcare secures all system interfaces and associated infrastructure to ensure confidentiality, integrity, and availability (CIA) of data during transmission and processing. Interfaces—including APIs, file exchanges, and integration points—are protected using: - Encryption in transit (e.g., TLS 1.2+ for HTTPS, SFTP) - Authentication and access controls to restrict use to authorized systems and users - Input validation and logging to detect unauthorized activity or anomalies - Availability safeguards such as monitoring, redundancy, and failover design All data exchanged through Modivcare's interfaces is encrypted using industry-standard protocols, and infrastructure components supporting those interfaces are monitored and hardened against vulnerabilities. These protections are implemented and reviewed under Modivcare's compliance frameworks, including SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701.
32	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall develop/integrate services using standardized Web Services formats.		Yes	Modivcare develops and integrates services using standardized web service formats, consistent with industry best practices and client interoperability requirements. Supported formats and protocols include: - RESTful APIs with JSON payloads (most commonly used) - SOAP with XML, where legacy or partner systems require it - Secure data transport over HTTPS/SFTP, in alignment with compliance standards Web services are designed to support consistent request/response structures, error handling, and authentication patterns. API documentation is maintained to support integration and onboarding. Modivcare's use of standardized formats ensures compatibility across systems and supports compliance with HIPAA, SOC 2 Type II, HITRUST r2, ISO 27001, and ISO 27701. If DHS has specific format or protocol preferences, Modivcare will review and align with those expectations following contract execution.
33	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall provide the ability to publish services and related data to be used by different types and classes of service consumers.		Yes	Modivcare provides the ability to publish services and related data for consumption by various internal and external systems, users, and partners. Services are exposed through standardized APIs, batch interfaces, or secure file exchanges, depending on the consumer's system type and integration model. Access is managed using: - Role-based permissions and authentication (e.g., API keys, token-based auth) - Data segmentation and filtering to ensure consumers access only the data they are authorized to view - Support for multiple service consumer types, including web applications, backend systems, external agencies, and healthcare partners Service definitions and payload structures are maintained in a consistent format to support interoperability. Upon contract execution, Modivcare will review DHS-specific consumer classifications and data access needs to ensure proper alignment. These capabilities are governed under Modivcare's compliance frameworks, including SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701.
34	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall provide the capabilities for a Real-Time (or near real-time) Integrated Enterprise where common data elements about the customers served (e.g., clients) and services rendered are easily shared across organizational units with appropriate adherence to State and Federal security and privacy restrictions.		Yes	Modivcare supports a real-time or near real-time integrated enterprise model through the use of secure, standards-based APIs and event-driven architecture. This enables timely data sharing of client information and service activity across systems and organizational units while maintaining strict adherence to HIPAA, 42 CFR Part 2, and applicable state privacy regulations. Key capabilities include: - Real-time and near real-time APIs for accessing and updating client, trip, eligibility, and scheduling data - Data normalization and mapping to support consistency across applications - Role-based access controls and data filtering to ensure only authorized entities access protected data - Encryption in transit and at rest, and full audit logging of access and changes These integrations are governed by Modivcare's compliance frameworks, including SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701. Upon contract execution, Modivcare will review DHS's specific integration and data exchange requirements to ensure alignment with enterprise architecture and security standards.

35	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall have the capability to implement synchronous and asynchronous program-to-program communication, moving messages between service oriented architecture (SOA) service consumer modules and service provider modules at runtime.		Yes	Modivcare supports both synchronous and asynchronous program-to-program communication between service consumer and provider modules at runtime. These interactions are managed using secure, standards-based integration patterns that support interoperability within a Service-Oriented Architecture (SOA) model. Capabilities include: - Synchronous communication through RESTful APIs using HTTPS and JSON, enabling real-time data exchange and service invocation - Asynchronous communication via event-driven mechanisms, secure batch interfaces (e.g., SFTP), and message queuing frameworks where applicable - Loose coupling of service components, enabling modular design and scalable runtime interactions - Monitoring and logging of message delivery and status for traceability and audit purposes Modivcare's integration architecture is governed under its certified compliance frameworks, including SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701. If DHS specifies preferred protocols or interface patterns, Modivcare will review and align with those requirements following contract execution.
36	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall have message and data formats that will be based on logical representations of business objects rather than native application data structures.		Yes	Modivcare's message and data exchange formats are designed around logical business objects (e.g., client profiles, trip requests, eligibility records) rather than native application data structures. This abstraction allows for clearer integration, better interoperability, and simplified maintenance across systems. Key features include: - Standardized API payloads that represent business-level entities, not database schemas - Data mappings and transformation layers that decouple internal storage formats from external interfaces - Consistent data contracts that align with business workflows and partner requirements - Support for schema evolution and versioning to accommodate changes in business logic without exposing system internals These practices support flexibility across diverse integration scenarios and are maintained under Modivcare's SDLC, with oversight from its compliance frameworks: SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701. Upon contract execution, Modivcare will review DHS-specific data modeling requirements and align published schemas accordingly.
37	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall avoid point-to-point integrations. Application integration, both internal and external, will go through the DHS Enterprise Service Bus/Data Integration Hub.		Yes	Modivcare supports modular, service-based integration architectures and avoids rigid point-to-point integrations whenever possible. Internal and external system communication is designed to use loosely coupled interfaces and standardized service contracts, supporting hub-and-spoke or service bus models. Modivcare's architecture allows for: - Abstraction of services to facilitate interoperability and scalability - Use of APIs, message queues, and file-based exchange that are integration-hub friendly - Routing, transformation, and orchestration through middleware or ESB frameworks where applicable - Avoidance of direct application-to-application dependencies, reducing integration complexity Upon contract execution, Modivcare will work with DHS to integrate through the Enterprise Service Bus (ESB) or Data Integration Hub, aligning with DHS's data flow governance, interface standards, and security protocols. These practices are maintained under Modivcare's compliance with SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701.
38	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution WSDLs developed for Arkansas will conform to the W3C standards for restful API development.		Yes	Modivcare develops APIs in accordance with W3C and industry-recognized RESTful web service standards, including the use of HTTP methods, resource-oriented URIs, and JSON-formatted payloads. While WSDLs traditionally apply to SOAP-based services, Modivcare's REST APIs follow current best practices for API design and documentation, including: - Use of OpenAPI/Swagger specifications (where applicable) - Adherence to W3C guidelines for web architecture and RESTful interaction - Clear and consistent request/response schemas that reflect logical business objects - Support for versioning, stateless communication, and secure transmission If Arkansas (DHS) requires formal interface definitions or specific schema documentation formats (e.g., WSDL-equivalent for REST APIs), Modivcare will review and align with those technical standards following contract execution, subject to system compatibility and integration planning. These practices are maintained under Modivcare's software development lifecycle and certified frameworks: SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701.
39	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution design will allow for the solution to continue to operate despite failure or unavailability of one or more individual technology solution components.		Yes	Modivcare's solution architecture is designed for resilience and high availability, ensuring continued operation even if one or more system components fail or become temporarily unavailable. Key design features include: - Redundant infrastructure for critical services (e.g., load-balanced application servers, replicated databases) - Cloud-based hosting in AWS, enabling auto-scaling, failover, and availability zone separation - Service decoupling and modular design, allowing isolated components to fail without disrupting the entire system - Monitoring and alerting, to detect issues early and trigger automated recovery or manual intervention These architectural principles ensure that system availability and performance remain stable during hardware failures, network interruptions, or maintenance events. Modivcare's approach is reviewed under its certified frameworks, including SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701. Upon contract execution, Modivcare will review DHS-specific availability expectations and incorporate them into operational planning and service continuity procedures.
40	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall have the ability to use standards-based communication protocols, such as TCP/IP, HTTP, HTTP/S and SMTP. Protocol bridging: The ability to convert between the protocol native to the messaging platform and other protocols, such as Remote Method Invocation (RMI), IIOP and .NET remoting.		Yes	Modivcare supports standards-based communication protocols including TCP/IP, HTTP, HTTPS, and SMTP across its systems, APIs, and integration layers. These protocols are used to securely transmit data between service components, partners, and platforms. Where needed, Modivcare supports protocol bridging to convert between internal messaging formats and external protocols. This may include: - API gateways or middleware handling protocol translation between RESTful HTTP interfaces and other formats - Integration adapters that enable compatibility with third-party or legacy systems - Use of modern frameworks that abstract or encapsulate legacy protocols (e.g., RMI, IIOP, or .NET remoting), if required These integration capabilities are implemented in line with Modivcare's compliance programs, including SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701. Modivcare will evaluate and support any DHS-specific protocol requirements or interoperability needs following contract execution, subject to technical feasibility and system compatibility.

41	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution will have the capability to work with security policy manager for Web services that allows for centrally defined security policies that govern Web services operations (such as access policy, logging policy, and load balancing).		Yes	Modivcare’s architecture supports the use of a centralized security policy manager to govern Web services operations. Web services are designed to integrate with security gateways or API management platforms that enable: - Access control policies based on roles, tokens, or API keys - Centralized logging and audit tracking for API transactions and access attempts - Load balancing and traffic management for high availability and performance - Policy enforcement points that apply rules for rate limiting, authentication, and authorization Security policies for Web services are defined and managed as part of Modivcare’s secure development lifecycle and are enforced through enterprise-grade API infrastructure. These practices align with Modivcare’s compliance programs under SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701. Modivcare will review and align with DHS’s security policy manager requirements following contract execution, including specific tooling or integration points as defined by the DHS Enterprise Platform.
42	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall have the capability to integrate with Master Data Management (MDM) technology for Enterprise Master Client Index (EMCI) implemented as part of the "State Hub" in a centralized or registry style implementation.		Yes	Modivcare supports integration with Master Data Management (MDM) systems, including centralized and registry-style implementations commonly used to manage client or member identity across enterprise systems. This includes the ability to: - Exchange and reconcile data with external identity management systems - Use standardized identifiers and crosswalks to support accurate data matching - Perform near real-time or scheduled updates through API- or batch-based integration - Apply validation and deduplication rules consistent with state-defined MDM logic - Maintain audit logging and ensure data exchange aligns with privacy and consent requirements Upon contract execution, Modivcare will review the specific architecture and integration model used within the Arkansas “State Hub” or equivalent enterprise client index, and will align with those requirements through Modivcare’s data governance and integration frameworks. These practices are managed under Modivcare’s certified compliance programs, including SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701.
43	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall be responsive and will automatically be sized for an optimum view to the display dimensions of PC, Tablet or Mobile phone.		Yes	Modivcare designs its web-based applications and portals using responsive design principles, ensuring that user interfaces automatically adjust to the display dimensions of PCs, tablets, and mobile devices. This is achieved through: - Flexible grid layouts and scalable UI components - CSS media queries and mobile-first design practices - Browser and device compatibility testing to validate functionality across platforms - Support for dynamic resizing and touch-based interactions These practices provide an optimized and accessible user experience regardless of device type or screen size. Modivcare’s front-end design standards are regularly reviewed and maintained under its product development lifecycle and governed by compliance frameworks including HIPAA, SOC 2 Type II, HITRUST r2, ISO 27001, and ISO 27701.
44	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution components will be committed to an advanced approach to interoperability using web services and Service Oriented Architecture (SOA) aligned with DHS Enterprise Architecture Standards and industry standards and vision for interoperability.		Yes	Modivcare is committed to an advanced, standards-based approach to interoperability, leveraging web services and Service-Oriented Architecture (SOA) principles to enable secure, scalable, and modular integration across enterprise systems. Key capabilities include: - RESTful and SOAP-based web services that support real-time and asynchronous communication - Modular service components that enable loose coupling and interface reuse across programs - Standard data formats and transport protocols (e.g., JSON, XML, HTTPS, SFTP) - API documentation and governance to support consistent integration with internal and external systems Modivcare's interoperability framework aligns with industry standards and can integrate with enterprise platforms and architectures used by government agencies. Upon contract execution, Modivcare will review and align with DHS Enterprise Architecture Standards and integration vision, subject to technical compatibility and system design requirements. These integration practices are supported under Modivcare’s certified compliance programs, including SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701.
45	General System Behavior	Perf. and Avail.	Any technology vendor, application or solution must be architected to support replication of the virtual machines to a secondary site.		Yes	Modivcare’s infrastructure is hosted in a cloud-based environment (AWS) that supports the replication of virtual machines and related workloads to a secondary site. Replication and redundancy are designed to ensure service continuity and data availability in the event of an outage or disaster. Key features include: - Multi-zone availability within AWS to support automatic failover - Snapshot-based backup and VM image replication to separate storage locations - Disaster recovery planning that includes infrastructure restoration and system redeployment - Scalable resource provisioning for rapid environment rebuild at a secondary site These capabilities are implemented and maintained under Modivcare’s disaster recovery and business continuity framework, which is reviewed as part of its compliance with SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701. Following contract execution, Modivcare will review DHS-specific recovery architecture and site requirements to confirm alignment with state DR objectives and infrastructure expectations.
46	General System Behavior	Perf. and Avail.	Any technology vendor, application or solution must be designed so all releases can be performed between 7pm and 6am except critical releases		Yes	Modivcare’s release management process is designed to support off-hours deployments, including release windows between 7:00 PM and 6:00 AM, in order to minimize disruption to users and business operations. Key features include: - Automated deployment pipelines that allow for controlled and scheduled releases - Change Advisory Board (CAB) approval to validate timing and impact - Support team coverage during release windows for monitoring and rollback readiness - Separation of emergency/critical release procedures, which can be executed outside standard windows if required Modivcare will coordinate with DHS to define release schedules, blackout periods, and escalation protocols during onboarding. This approach aligns with Modivcare’s SDLC and is governed under its compliance programs including SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701.

47	General System Behavior	Perf. and Avail.	Any technology vendor, application or solution shall leverage virtualization to expedite disaster recovery. Virtualization enables system owners to quickly reconfigure system platforms without having to acquire additional hardware.		Yes	Modivcare leverages virtualized infrastructure within a cloud-hosted environment to support rapid recovery and reconfiguration of system platforms in the event of a disaster. This eliminates the need for acquiring additional physical hardware and significantly reduces recovery time. Key disaster recovery benefits enabled by virtualization include: - Rapid provisioning of virtual machines (VMs) from pre-defined templates or snapshots - Flexible reallocation of compute and storage resources to restore services in alternate zones or environments - Automated failover and recovery workflows using cloud-native orchestration - Infrastructure-as-code practices for consistent and repeatable recovery deployments These capabilities are integrated into Modivcare's business continuity and disaster recovery framework, which is reviewed and tested regularly under compliance programs including SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701.
48	General System Behavior	Perf. and Avail.	Any technology vendor, application or solution will provide the ability to perform archival/incremental backups and the ability to perform open/closed database backups.			Modivcare's backup strategy includes support for both archival and incremental backups, as well as the ability to perform open and closed database backups depending on the system state and operational requirements. Key capabilities include: - Incremental and full backups scheduled based on data criticality and retention policies - Archival storage for long-term data preservation in encrypted, access-controlled environments - Support for open database backups (while systems remain online) using hot-backup tools and snapshot technologies - Support for closed (offline) database backups during maintenance windows or where required by system type or policy Automated backup integrity checks and monitoring to validate success and support recoverability These practices are governed under Modivcare's enterprise backup and disaster recovery procedures, reviewed regularly as part of its compliance with SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701.
49	General System Behavior	Perf. and Avail.	Any technology vendor, application or solution will provide at least one (1) production and one (1) non-production environment. Highly available solutions that mitigate single points of failure are recommended and encouraged.		Yes	Modivcare supports the deployment of production and non-production environments—including development, testing, and staging—as required by the project scope and operational needs. Environments are logically separated to preserve data integrity, enforce access control, and prevent cross-environment impact. The production environment is architected for high availability, with: - Redundant infrastructure across multiple availability zones - Load balancing and failover mechanisms to eliminate single points of failure - Monitoring, alerting, and automated recovery processes to ensure continuity - Backup and disaster recovery procedures aligned with compliance expectations Modivcare will work with DHS to define environment provisioning and availability expectations following contract execution, ensuring full alignment with program and SLA requirements. All environment controls are governed under Modivcare's certified compliance frameworks: SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701.
50	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall allow for different roles for Users including Operators, Administrators, Managers etc.		Yes	Modivcare's systems support role-based access control (RBAC) to ensure that users are granted permissions based on their specific roles and responsibilities. Common user roles include Operators, Administrators, Managers, and others as defined by business needs or contractual requirements. Key features include: - Granular role definitions to control access to data, functions, and system modules - Separation of duties, ensuring sensitive actions (e.g., user provisioning, audit review) are restricted to authorized roles - Centralized access management with approval workflows for role assignments - Auditing and logging of user actions based on assigned roles These access control practices are governed under Modivcare's compliance with SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701. Role definitions can be configured to align with DHS-specific operational and security requirements following contract execution.
51	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall, at a minimum, provide a mechanism to comply with security requirements and safeguard requirements of the following Federal agencies / entities: a. Health & Human Services (HHS) Centers for Medicare & Medicaid Services (CMS) b. Guidance from CMS including MITA Framework 3.0 and Harmonized Security and Privacy Framework c. Administration for Children & Families (ACF) d. Dept. of Agriculture Food and Nutrition Services e. NIST 800-53 r5 Moderate, MARS-E and DOD 8500.2 f. IRS pub 1075, which points back to NIST 800-53 rev 3 g. Federal Information Security Management Act (FISMA) of 2002 h. Health Insurance Portability and Accountability Act (HIPAA) of 1996 i. Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009 j. Privacy Act of 1974 k. e-Government Act of 2002 l. Patient Protection and Affordable Care Act of 2010, Section 1561 Recommendations m. Section 471(a)(8) of the Social Security Act n. Section 106(b)(2)(B)(viii) of the Child Abuse Prevention and Treatment Act		Yes	Modivcare maintains a robust information security and privacy program that aligns with applicable federal and regulatory standards governing healthcare, human services, and public sector data protection. This program is independently assessed under the following certified frameworks: - SOC 2 Type II, covering security, availability, and confidentiality - HIPAA and HITECH, addressing healthcare privacy and breach safeguards - HITRUST r2, which maps to NIST, CMS, and state/federal data protection standards - ISO/IEC 27001:2022 and ISO/IEC 27701:2019, governing information security and privacy management While Modivcare is not directly certified against all listed federal frameworks, its control environment is aligned to and maps with components of: - NIST 800-53 rev 5 (moderate baseline) - MARS-E (Minimum Acceptable Risk Standards for Exchanges) - IRS Pub 1075 - Applicable federal laws such as the Privacy Act of 1974, FISMA, and the e-Government Act Modivcare continuously reviews its security practices to ensure they meet evolving compliance expectations. Upon contract execution, Modivcare will work with DHS to evaluate specific interpretations of these requirements and ensure alignment with DHS enterprise security standards and applicable state or federal mandates.
52	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall adhere to the accessibility standard as outlined in the web guidelines and based on the W3C level 2 accessibility guidelines: (http://www.w3.org/TR/WCAG10/full-checklist.html)		Yes	Modivcare designs and maintains its public-facing and stakeholder-accessible websites and portals in alignment with Web Content Accessibility Guidelines (WCAG) published by the W3C, targeting compliance with WCAG 2.0 Level AA standards or better. Key accessibility practices include: - Support for screen readers and assistive technologies - Keyboard navigability and focus management for non-mouse users - Use of alt text, semantic HTML, and readable structure - Color contrast and font size adherence for readability Accessibility features are validated through internal quality assurance processes and tools that evaluate conformance to WCAG success criteria. Modivcare also complies with related state and federal accessibility regulations (e.g., Section 508 and applicable state web standards), as required by contractual obligations. Upon contract execution, Modivcare will review any DHS-specific accessibility policies and ensure the solution aligns with W3C Level 2 (WCAG 2.0 AA) and any referenced state-specific accessibility expectations.

53	General System Behavior	Regulatory & Usability	Any technology vendor, application or solution shall adhere to the AR State accessibility standards and comply with the provisions of Arkansas Code Annotated § 25-26-201 et seq., as amended by Act 308 of 2013.		Yes	Modivcare is committed to supporting accessibility across its platforms and aligning with applicable state and federal accessibility standards. Modivcare currently incorporates WCAG 2.0 Level AA design principles, supports assistive technologies, and performs accessibility validation as part of its standard development lifecycle. Modivcare will review the Arkansas State accessibility standards and Arkansas Code Annotated § 25-26-201 et seq., as amended by Act 308 of 2013, to determine applicability and confirm alignment with program requirements following contract execution, subject to internal review and integration planning. Accessibility compliance is governed under Modivcare's certified frameworks, including SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701.
54	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution comply with the DHS branding standards as defined by DHS.		Yes	Modivcare will review and, where appropriate, align with DHS-defined branding standards for technology solutions including logos, color schemes, templates, content formatting, and user interface elements following contract execution and upon receipt of DHS's official branding requirements. Modivcare has experience implementing client-specific branding in state, federal, and commercial programs and will coordinate with DHS to ensure any branding adjustments are scoped, reviewed, and incorporated as part of the implementation process, subject to internal design and compliance review.
55	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall adhere to the principle of "Fail Safe" to ensure that a system in a failed state does not reveal any sensitive information or leave any access controls open for attacks		Yes	Modivcare adheres to the principle of fail-safe security, ensuring that systems in a failed or degraded state do not expose sensitive information or leave access controls in an insecure condition. Key safeguards include: - Default-deny configurations for authentication and access if systems fail to validate credentials or permissions - Session and token expiration logic that prevents access continuation after failure or timeout - Application and infrastructure hardening to restrict debug output, stack traces, or unintended data exposure during faults - Monitoring and alerting to detect system exceptions and enforce automated containment These practices are integrated into Modivcare's secure development lifecycle and operations framework, and regularly reviewed under its compliance programs: SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701. Upon contract execution, Modivcare will collaborate with DHS to validate any additional fail-safe requirements specific to its environment or data classification.
56	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of information		Yes	Modivcare maintains a risk-based security program that aligns the level of protection with the sensitivity of the information and the potential impact of loss, misuse, unauthorized disclosure, or modification. Security controls are implemented based on: - Data classification and risk assessment results - Threat modeling and impact analysis performed during solution design and ongoing operations - Least privilege and role-based access controls to minimize exposure - Encryption, audit logging, and incident response procedures tailored to data criticality - Continuous compliance monitoring through independently audited frameworks: - SOC 2 Type II - HIPAA - HITRUST r2 - ISO 27001 and ISO 27701 Modivcare's approach ensures that technical and administrative safeguards are commensurate with the risk and potential harm to affected stakeholders and data assets. Upon contract execution, Modivcare will review any DHS-specific data handling and classification requirements to confirm appropriate control alignment.
57	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall follow the DHS Enterprise Architecture Standards regarding identity, authorization and access management. The current standards state that applications/solutions will integrate with Microsoft's Active Directory for internal/DHS users and will integrate with the IBM Cloud Identity platform for external users. Modern authentication protocols such as SAML or OIDC should be used and multi-factor authentication will be employed whenever deemed necessary by DHS or applicable regulatory bodies (CMS, FNS, IRS, etc.).		Yes	Modivcare supports federated identity, role-based access control, and multi-factor authentication across its solutions and is prepared to integrate with DHS's identity and access management standards, subject to technical alignment and scope confirmation. Modivcare's systems support: - Integration with Microsoft Active Directory (AD) for internal identity management - Standards-based authentication protocols, including SAML 2.0 and OpenID Connect (OIDC) - Multi-factor authentication (MFA), configurable based on user roles, risk context, or regulatory requirements - External identity provider integration, including platforms such as IBM Cloud Identity, through supported federation protocols Upon contract execution, Modivcare will review DHS's specific IAM configuration—including AD integration for internal users and IBM Cloud Identity for external users—and align authentication workflows accordingly, subject to feasibility and onboarding requirements. These identity controls are governed under Modivcare's compliance frameworks: SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701.
58	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall support protection of confidentiality of all Protected Health Information (PHI) and Personally Identifiable Information (PII) delivered over the Internet or other known open networks via supported encryption technologies needed to meet CMS and NIST requirements for encryption of PHI and PII data. Examples include: Advanced Encryption Standard (AES) and an open protocol such as Transport Layer Security (TLS), Secure Sockets Layer (SSL), Internet Protocol Security (IPsec), XML encryptions, or Secure/Multipurpose Internet Mail Extensions (S/MIME) or their successors. All vendors, applications and solutions will be subject to external Audit checks.		Yes	Modivcare safeguards all Protected Health Information (PHI) and Personally Identifiable Information (PII) transmitted over the internet or open networks using encryption technologies aligned with CMS, NIST, and HIPAA requirements. Encryption practices include: - TLS 1.2+ for secure transmission of data across web services, portals, and file exchanges - AES-256 for data at rest, using cloud-native encryption tools - Secure email and file transfer mechanisms, such as S/MIME, SFTP, and secure portals - Use of FIPS 140-2 validated cryptographic modules, where supported by Modivcare's underlying infrastructure, including cloud-hosted services (e.g., AWS) - Role-based access controls and detailed audit logging to preserve confidentiality and traceability These safeguards are implemented as part of Modivcare's enterprise security and compliance program and are regularly assessed through internal reviews and external audits tied to its certifications: SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701. Following contract execution, Modivcare will review and align with any DHS-specific encryption protocols or platform integration requirements.

59	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall, when storing PHI/PII, support the use of encryption technologies needed to meet CMS and NIST requirements for the encryption of PHI/PII data at rest.		Yes	Modivcare encrypts all Protected Health Information (PHI) and Personally Identifiable Information (PII) at rest using encryption technologies that align with CMS and NIST standards for protecting sensitive data. Encryption at rest is implemented using: - AES-256 encryption, consistent with NIST Special Publication 800-111 and CMS MARS-E guidelines - Cloud-native encryption services that support secure key management, access controls, and automated encryption enforcement - NIST-recommended cryptographic algorithms, and, where applicable, infrastructure components that may support FIPS 140-2 validated modules, depending on system configuration and deployment context - Access logging, key management, and role-based access controls to enforce confidentiality and data protection policies These controls are reviewed and validated under Modivcare's enterprise compliance program, including certifications for SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701.
60	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution, prior to accessing any PHI, display a State-approved configurable warning or login banner (e.g. "The System should only be accessed by authorized users"). In the event that a application or solution does not support pre-login capabilities, the application or solution will display the banner immediately following authorization.		Yes	Modivcare supports the display of configurable login or post-login banners designed to communicate authorized use requirements prior to accessing systems containing PHI. Where technically feasible, these banners can be shown before user authentication; otherwise, they are displayed immediately upon successful login. Modivcare can accommodate state-provided or approved banner language (e.g., "This system may only be accessed by authorized users") subject to platform compatibility and technical configuration review. This functionality is managed as part of Modivcare's standard implementation process and is supported under its broader compliance programs, including HIPAA, SOC 2 Type II, HITRUST r2, ISO 27001, and ISO 27701. Final placement and message content would be reviewed and addressed following contract execution, in accordance with system constraints and DHS policy alignment.
61	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall not transmit or store any Personal Health Information (PHI) or Personally Identifiable Information (PII) using publically available storage over the Internet or any wireless communication device, unless: 1) the PHI or PII is "de-identified" in accordance with 45 C.F.R § 164.514(b) (2); or 2) encrypted in accordance with applicable law, including the American Recovery and Reinvestment Act of 2009 and as required by policies, procedures and standards established by DHS		Yes	Modivcare does not transmit or store PHI or PII using publicly available internet-based or wireless storage platforms unless appropriate safeguards are in place. Specifically, PHI/PII is only stored or transmitted when: It has been de-identified in accordance with 45 C.F.R. § 164.514(b)(2) or It is encrypted using NIST-recommended algorithms, such as AES-256 for data at rest and TLS 1.2+ for data in transit, consistent with HIPAA and HITECH privacy and security provisions Modivcare implements additional safeguards including: - Access control and authentication policies - Encryption key management - Audit logging - Mobile and wireless protection policies, where applicable These practices are reviewed regularly as part of Modivcare's enterprise security and compliance program and audited under frameworks including SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701.
62	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution will include the same security provisions for the development, System test, Acceptance test and training environment as those used in the production environment except those provisions implemented specifically to protect confidential information (e.g. PHI, PII).		Yes	Modivcare applies the same core security provisions across its development, system test, acceptance test, and training environments as those used in production, with the exception of controls specifically tied to the protection of live PHI or PII. Security controls consistently applied across environments include: - User authentication and access controls - Network and endpoint security configurations - Vulnerability management and patching - Audit logging and activity monitoring - Environment isolation and least-privilege access enforcement Live PHI and PII are not used in non-production environments. When test data is required, Modivcare uses synthetic or de-identified data, and additional technical safeguards (e.g., obfuscation or masking) are implemented as needed. These environment protections are governed under Modivcare's security and compliance program and are regularly reviewed under its certifications: SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701.
63	general System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall be able to associate permissions with a user using one or more of the following access controls: a. Role-Based Access Controls (RBAC; users are grouped by role and access rights assigned to these groups) b. Context-based (role-based with additional access rights assigned or restricted based on the context of the transaction such as time-of-day, workstation-location, emergency-mode, etc.)		Yes	Modivcare supports Role-Based Access Control (RBAC) and has the capability to implement context-based access controls where needed to enforce security and privacy based on user responsibilities and transaction context. Key capabilities include: RBAC: Users are assigned roles based on their job function, with access rights granted to those roles. This ensures least-privilege access and separation of duties across administrative, operational, and support users. Context-based access (where supported): Additional controls may restrict or permit access based on factors such as time of day, user location, device type, or operational state (e.g., emergency or break-glass scenarios), particularly for administrative or privileged actions. These access control mechanisms are integrated into Modivcare's identity and access management framework and reviewed as part of ongoing compliance activities under HIPAA, SOC 2 Type II, HITRUST r2, ISO 27001, and ISO 27701. Modivcare will review and align access control configurations with DHS-specific policies and operational use cases following contract execution.
64	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution will comply with accessibility requirements described in 45 CFR 85 and with State of Arkansas accessibility requirements		Yes	Modivcare designs its web-based applications and user-facing platforms to align with federal accessibility requirements, including those described in 45 CFR Part 85, which implements Section 504 of the Rehabilitation Act, and the State of Arkansas accessibility standards, including Arkansas Code Annotated § 25-26-201 et seq., as amended. Key accessibility features include: - Conformance with WCAG 2.0 Level AA guidelines - Support for screen readers, keyboard navigation, and assistive technologies - Alternative text, logical tab order, and consistent UI structures - Device-responsive design for accessibility across PC, tablet, and mobile platforms Modivcare will review and incorporate DHS-specific accessibility requirements during implementation planning, subject to technical feasibility and interface compatibility. These accessibility practices are managed under Modivcare's SDLC and quality assurance program and align with its compliance frameworks, including SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701.

65	General System Behavior	Solution Administration	Any technology vendor, application or solution will allow System administrators to create and manage user roles.		Yes	Modivcare's platforms support the ability for authorized system administrators to create, assign, and manage user roles and associated access permissions based on operational needs and security policies. Key capabilities include: - Role-Based Access Control (RBAC): Roles are defined based on job functions, with corresponding access rights - Administrative interfaces allow authorized personnel to add, modify, deactivate users, and assign or update role memberships - Audit logging of role assignments and user access changes to support accountability and compliance - Segregation of duties and least privilege principles applied in role design and administrative functions User role management is governed under Modivcare's identity and access management policies and is reviewed regularly through audits aligned with SOC 2 Type II, HIPAA, HITRUST r2, ISO 27001, and ISO 27701.
66	General System Behavior	Solution Administration	Any technology vendor, application or solution communications will be protected by at least 256-bit encryption.		Yes	Modivcare protects all system communications using 256-bit encryption algorithms, such as AES-256 for data at rest and TLS 1.2 or higher for data in transit. This level of encryption meets or exceeds industry standards for protecting PHI and PII in compliance with HIPAA, NIST, and related regulatory frameworks.
67	General System Behavior	Solution Administration	Any technology vendor, application or solution will be supported by public key/private key encryption Secure Socket Layer (SSL) certificates.		Yes	Modivcare uses TLS (successor to SSL) protocols with public/private key encryption certificates issued by trusted Certificate Authorities (CAs). These are implemented across all secure web applications, APIs, and file transfer services to ensure authenticated, encrypted connections and protection against interception or tampering.
68	General System Behavior	Regulatory & Usability	Any application or solution will use colors to enhance user experience and System usability while complying with all disability requirements notated elsewhere in these requirements.		Yes	Modivcare's user interface design applies color schemes that enhance usability and accessibility, while aligning with WCAG 2.0 Level AA guidelines and applicable Section 508 and Arkansas accessibility requirements. This includes ensuring sufficient color contrast, avoiding color-only cues, and supporting screen readers and keyboard navigation where required.
69	General System Behavior	User Interrace	Any technology vendor, application or solution must perform address validation for demographic information (e.g., USPS, Smarty Streets, AR GIS, etc.). Suggest the validated new address and prompt user to select either user entered address or validated address and then save accordingly.		Yes	Modivcare supports address validation integrations with third-party services (e.g., USPS, SmartyStreets) for confirming and formatting demographic address data. The system can suggest validated addresses to users, compare them with the originally entered address, and allow the user to select the preferred version before saving.
70	General System Behavior	User Interface	Any technology vendor, application or solution must perform standard data validations such as character, numeric, date, currency , phone, SSN etc.		Yes	Modivcare platforms incorporate standard field-level data validations to ensure data integrity and input accuracy. Validations include checks for character limits, numeric formats, date structures, currency symbols and precision, phone number formatting, and SSN structure validation based on defined patterns. These validations are enforced at both client-side and server-side layers where appropriate.
71	General System Behavior	User Interlace	Any technology vendor, application or solution must have the ability to auto-save, prompt to save when leaving pages in all modules.		Yes	Modivcare's applications support auto-save functionality and user prompts to reduce data loss during navigation or inactivity. When users attempt to leave a module or form with unsaved changes, configurable alerts notify them to save or confirm the action. This helps ensure data completeness and prevents accidental loss of input.
72	General System Behavior	User Interlace	Any technology vendor, application or solution shall have the ability to create prompts for user actions. (e.g., incomplete data entry of required fields, deletion of data, system log-off warnings).		Yes	Modivcare platforms support interactive prompts for key user actions, including but not limited to: Incomplete form submissions Confirmation for data deletion Session timeout or log-off alerts These prompts enhance usability and reduce risk of unintended actions or incomplete transactions.
73	General System Behavior	User Interlace	Any technology vendor, application or solution shall have the capability to send notifications. Examples include sending emails, text messages (SMS), etc.		Yes	Modivcare's systems support multi-channel notifications, including email, SMS (text), and in-platform alerts. Notifications can be event-driven (e.g., appointment reminders, system updates) and are configurable based on user role and business requirements. These capabilities support both internal workflows and external communication with members, facilities, and partners.
74	General System Behavior	Web based UI	Any technology vendor, application or solution providing data over a web browser interface (http, ftp, etc.) will include the capability to encrypt the data communicated over the network via SSL (e.g.. HTML over HTTPS).		Yes	Modivcare encrypts all data transmitted over web browser interfaces using TLS (the successor to SSL) to secure communication channels. Web portals, APIs, and file transfer services are configured to operate over HTTPS and SFTP, ensuring encrypted data exchange in compliance with industry standards such as HIPAA and NIST guidelines.
75	General System Behavior	Web based UI	The system will support and maintain compatibility with the current to (N-2) version of the DHS Support Operating Systems. The supported Operating Systems are Microsoft Windows, MAC OS, Apple IOS and Google Android.		Yes	Modivcare designs and tests its web and mobile applications to maintain compatibility with the current and two prior versions (N-2) of major supported operating systems, including: Microsoft Windows macOS Apple iOS Google Android User-facing applications follow responsive design principles and undergo multi-platform validation as part of Modivcare's quality assurance processes.
76	General System Behavior	Web based UI	The system will support and maintain compatibility with the current to (N-2) version of the DHS approved Browsers. The supported Browsers are Chrome, Edge, and Safari. This is to ensure that vendors test and certify their software/application for current to (N-2) versions of these Browsers.		Yes	Modivcare designs and tests its web-based applications to maintain compatibility with the current and two prior (N-2) versions of Google Chrome, Microsoft Edge, and Apple Safari. Cross-browser functionality is validated through QA processes and regression testing to ensure a consistent user experience across supported DHS browser environments.
77	Technology Platform Requirements	Data Integ,Quality, ETL	Any technology vendor, application or solution Extract Transform and Load (ETL) components will provide process flow and user interface capabilities to enable business users to perform data-quality-related tasks and fulfill stewardship functions, including: a. Packaged processes, including steps used to perform common quality tasks (providing values for incomplete data, resolving conflicts of duplicate records, specifying custom rules for merging records, profiling, auditing, for example) b. User interface in which quality processes and issues are exposed to business users, stewards and others c. Functionality to manage the data quality issue resolution process through the stewardship workflow (status tracking, escalation and monitoring of the issue resolution process) d. Ability to customize the user interface and workflow of the resolution process e. Ability to execute data quality resolution steps in the context of a process orchestrated by Business Process Management (BPM) tools (packaged integration or other ability to work with popular BPM suites, for example)		Yes	Modivcare's data integration platforms support ETL capabilities that enable data quality management and stewardship workflows. These include: a. Packaged processes for handling incomplete, duplicate, or conflicting records, with configurable business rules for merging, profiling, and validation b. User interfaces that expose quality issues and data flags to business users, data stewards, and other stakeholders c. Status tracking and escalation tools to manage data issue resolution workflows, including audit trails and resolution monitoring d. Interface and workflow customization options to adapt data remediation processes based on operational needs e. Integration capability with Business Process Management (BPM) tools to