



STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
DIVISION OF LONG TERM SUPPORTS AND SERVICES

Lori A. Shibinette
Commissioner

Melissa A. Hardy
Director

105 PLEASANT STREET, CONCORD, NH 03301
603-271-5034 1-800-852-3345 Ext. 5034
Fax: 603-271-5166 TDD Access: 1-800-735-2964
www.dhhs.nh.gov

September 2, 2022

His Excellency, Governor Christopher T. Sununu
and the Honorable Council
State House
Concord, New Hampshire 03301

REQUESTED ACTION

Authorize the Department of Health and Human Services, Division of Long Term Supports and Services, to enter into a contract with FDGS, Limited Partnership, a/k/a First Data Government Solutions, Limited Partnership (VC #TBD), Brookfield, WI, in the amount of \$1,700,000 for the provision of an Electronic Visit Verification (EVV) System for all Medicaid personal care services (PCS) and home health care services (HHCS) that require an in-home visit by a provider, with the option to renew for up to four (4) additional years, effective upon Governor and Council approval through June 30, 2026. 79% Federal Funds, 21% General Funds.

Funds are available in the following accounts for State Fiscal Year 2023, and are anticipated to be available in State Fiscal Years 2024, 2025, and 2026, upon the availability and continued appropriation of funds in the future operating budget, with the authority to adjust budget line items within the price limitation and encumbrances between state fiscal years through the Budget Office, if needed and justified.

05-95-48-480030-9318-034-500099 HEALTH AND SOCIAL SERVICES, DEPT OF HEALTH AND HUMAN SVCS. HHS: ELDERLY AND ADULT SERVICES, STATE OFFICE ADMIN, ELECTRONIC VISIT VERIFICATION SYSTEM

State Fiscal Year	Class / Account	Class Title	Job Number	Total Amount
2023	034-500099	Major IT Systems	New	\$503,000
			Subtotal	\$503,000

05-95-47-470010-8009-102-500731 HEALTH AND SOCIAL SERVICES, HEALTH AND HUMAN SVCS DEPT, HHS: OFC MEDICAID SERVICES, DIVISION OF MEDICAID SERVICES, MEDICAID MANAGEMENT INFORMATION SYSTEM

State Fiscal Year	Class / Account	Class Title	Job Number	Total Amount
2024	102-500731	Contracts for Prog SVC	New	\$399,000
2025	102-500731	Contracts for Prog SVC	New	\$399,000
2026	102-500731	Contracts for Prog SVC	New	\$399,000
			Subtotal	\$1,197,000
			Total	\$1,700,000

26 mac

EXPLANATION

The purpose of this request is to implement an Electronic Visit Verification System for all Medicaid personal care services and home health care services that require an in-home visit by a provider. Electronic visit verification for these services is required by Section 1903 of the Social Security Act (42 U.S.C. 1396b), also known as the 21st Century Cures Act. To bring the Department into compliance with the 21st Century Cures Act, the Department is required to implement electronic visit verification for in-home personal care services and in-home home health services by January 1, 2023. States that do not comply with these regulations are subject to fines equal to 1% of eligible expenditures.

The focus of the Electronic Visit Verification are those services provided through a home visit in the person's home. Electronic Visit Verification is not required for services outside of a person's home, for those provided by a family member, or 24/7 residential services. With the provision of services delivered in the home there is a federal requirement to ensure that care is being delivered as specified by the care plan and authorized by the Department; and that publicly funded resources are being managed and spent appropriately. The Electronic Visit Verification System will capture the six data elements required by the 21st Century Cures Act for home-based personal care services and home health care service member visits including:

1. the member receiving the service
2. type of service
3. date of service
4. location of service delivery
5. the direct care worker providing the service, and
6. worker check in/check out times

Goals and objectives for the Electronic Visit Verification System are to:

- Ensure individuals receive the services they are authorized to receive;
- Comply with the requirements within the 21st Century Cures Act;
- Provide data to support quality improvement and program efficiencies;
- Provide the Department with the ability to view utilization of services in real time;
- Improve the quality of care for recipients receiving services paid for with Medicaid funds;
- Reduce unauthorized services and billing errors, and improve payment accuracy; and
- Provide additional auditing tools to reduce fraud, waste and abuse.

Approximately 145 contracted service providers will use the Electronic Visit Verification System, and they will serve approximately 15,000 individuals and families annually.

The Contractor will provide a commercial off-the-shelf electronic visit verification system that will meet the requirements set forth in the 21st Century Cures Act and the needs of the Department, the individuals they serve, service recipients' families, and service providers. The Electronic Visit Verification System will support all members who receive services delivered in their home, including those who utilize member-directed personal care service models, and be designed in such a way that it does not hinder the ability of individuals and/or families receiving services to schedule services or choose where they receive their services. The Electronic Visit Verification System is a secure system designed to protect the member's privacy. The Electronic Visit Verification System will be able to report on key performance indicators.

The Department will monitor the Contractor's performance with the following key performance measures:

- The Contractor's solution must be available twenty four (24) hours a day, 7 days a week, except during scheduled maintenance periods.
- The Contractor must provide a real-time performance monitoring dashboard that is available ninety-nine percent (99%) of the time, twenty-four (24) hours a day, seven (7) days a week, excluding Department-approved planned downtime.
- The Contractor must ensure that the data integrity error rate and routing errors of transactions is less than .001%.
- The Contractor must ensure all standardized reports are available online or delivered to authorized users by the scheduled time 100% of the time.
- The Contractor must ensure the Electronic Visit Verification system provides the capability to exchange and interface data with systems of record and process updates in near real time (within three (3) seconds, 99% of the time).
- The Contractor's help desk must answer all calls within two (2) minutes or less of the call entering the queue, as determined based on the monthly average.

The Department selected the Contractor through a competitive bid process using a Request for Proposals (RFP) that was posted on the Department's website from December 14, 2021 through March 8, 2022. The Department received five (5) responses that were reviewed and scored by a team of qualified individuals. The Scoring Sheet is attached.

As referenced in Exhibit A, Special Provisions, Section A.1 of the attached agreement, the parties have the option to extend the agreement for up to four (4) additional years, contingent upon satisfactory delivery of services, available funding, agreement of the parties, and Governor and Council approval.

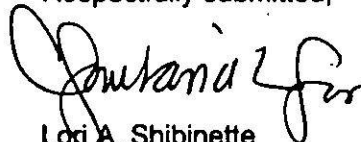
Should the Governor and Council not authorize this request, the Department will not be able to comply with the requirements of the 21st Century Cures Act for in-home visit verification and will be required to pay CMS penalties that will exceed the cost of this contract. The CMS penalties include a reduction in the Federal Medical Assistance Percentage up to 1% for services that require EVV.

Area served: Statewide

Source of Federal Funds: Assistance Listing Number #93.778, FAIN #2105NH5ADM.

In the event that the Federal Funds become no longer available, General Funds will not be requested to support this program.

Respectfully submitted,



Lori A. Shibinette
Commissioner

New Hampshire Department of Health and Human Services
Division of Finance and Procurement
Bureau of Contracts and Procurement
Scoring Sheet

Project ID # RFP-2022-DLTSS-05-ELECT

Project Title Electronic Visit Verification System

	Maximum Points Available	CareBridge Medical Group, P.C.	First Data	Netsmart	Sandata	Therap Services
Technical						
Proposed Software Solution	150	120	140	100	135	100
Project Management Experience	100	85	95	75	90	65
Vendor Company	50	35	50	30	45	35
Staffing Qualifications	50	40	50	35	45	30
Subtotal - Technical	350	280	335	240	315	230
Cost						
Price Proposal	150	150	150	0	111	0
Subtotal - Cost	150	150	150	0	111	0
TOTAL POINTS	500	430	485	240	426	230
TOTAL PROPOSED VENDOR COST		\$1,710,000	\$1,700,000	\$10,044,857	\$2,290,000	\$1,256,938

Reviewer Name	Title
1 Wendi Aultman	BEAS Bureau Chief
2 Jane Hybsch	Medicaid Medical Services Admin.
3 Karen Carleton	Program Integrity Administrator
4 Roger Boissonneau	MMIS Director
5 Ken Gagne	MMIS Technology Manager
6 Grant Beckman	BIS Financial Manager
7 Kerri King	DLTSS Information Technology Manager



STATE OF NEW HAMPSHIRE
DEPARTMENT OF INFORMATION TECHNOLOGY
27 Hazen Dr., Concord, NH 03301
Fax: 603-271-1516 TDD Access: 1-800-735-2964
www.nh.gov/doit

Denis Goulet
Commissioner

September 7, 2022

Lori A. Shibinette, Commissioner
Department of Health and Human Services
State of New Hampshire
129 Pleasant Street
Concord, NH 03301

Dear Commissioner Shibinette:

This letter represents formal notification that the Department of Information Technology (DoIT) has approved your agency's request to enter into a contract with First Data Government Solutions, LP, of Brookfield, WI, as described below and referenced as DoIT No. 2022-031.

The purpose of this request is to implement an Electronic Visit Verification System for all Medicaid personal care services and home health care services that require an in-home visit by a provider. Electronic visit verification for these services is required by Section 1903 of the Social Security Act (42 U.S.C. 1396b), also known as the 21st Century Cures Act. The Department is required to implement electronic visit verification for in-home personal care services to bring the Department into compliance with the 21st Century Cures Act, and electronic visit verification is required for in-home home health services by January 1, 2023.

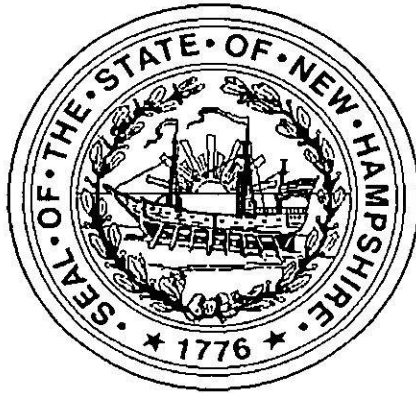
This contract includes a not to exceed spend amount of \$1,700,000.00 and shall become effective upon Governor and Executive Council approval through June 30, 2026.

A copy of this letter should accompany your Agency's submission to Governor and Executive Council for approval.

Sincerely,

Denis Goulet

DG/RA
DoIT #2022-031
cc: Michael Williams, IT Manager, DoIT



STATE OF NEW HAMPSHIRE

The Department of Health and Human Services

Electronic Visit Verification System

RFP-2022-DLTSS-05-ELECT -01- 2022-031

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
STATE OF NEW HAMPSHIRE GENERAL PROVISIONS - P37

Contents

EXHIBIT A - SPECIAL PROVISIONS.....	9
EXHIBIT B – STATEMENT OF WORK (SOW) BUSINESS AND TECHNICAL REQUIREMENTS AND DELIVERABLES.....	14
EXHIBIT C – PRICE AND PAYMENT SCHEDULE.....	52
1. CONTRACT PRICE.....	52
2. TRAVEL EXPENSES.....	52
3. SHIPPING FEES.....	52
4. INVOICING.....	52
5. INVOICE ADDRESS.....	52
6. PAYMENT ADDRESS.....	53
7. OVERPAYMENTS TO THE CONTRACTOR.....	53
8. CREDITS.....	53
9. RESERVED.....	53
10. PAYMENT SCHEDULE.....	53
EXHIBIT D – SOFTWARE AGREEMENT.....	59
1. LICENSE GRANT.....	59
2. SOFTWARE TITLE.....	61
3. SOFTWARE AND DOCUMENTATION COPIES.....	61
4. RESTRICTIONS.....	61
5. VIRUSES.....	61
6. AUDIT.....	61
7. SOFTWARE NON-INFRINGEMENT.....	62
8. CONTROL OF ALL COMPONENT ELEMENTS.....	63
9. CUSTOM SOURCE CODE.....	63
10. SOFTWARE ESCROW.....	63
EXHIBIT E – ADMINISTRATIVE SERVICES.....	65
1. DISPUTE RESOLUTION.....	65
2. ACCESS AND COOPERATION.....	65
3. RECORD RETENTION.....	66
4. ACCOUNTING.....	66
5. AUDIT.....	66

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
STATE OF NEW HAMPSHIRE GENERAL PROVISIONS - P37

6. MISCELLANEOUS WORK REQUIREMENTS66

EXHIBIT F – TERMS AND DEFINITIONS.....67

EXHIBIT G – ATTACHMENTS AND CONTRACTOR CERTIFICATES..... 72

1. ATTACHMENTS..... 72

2. CONTRACTOR CERTIFICATES..... 72

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
STATE OF NEW HAMPSHIRE GENERAL PROVISIONS - P37

FORM NUMBER P-37 (version 12/11/2019)

Notice: This agreement and all of its attachments shall become public upon submission to Governor and Executive Council for approval. Any information that is private, confidential or proprietary must be clearly identified to the agency and agreed to in writing prior to signing the contract.

AGREEMENT

The State of New Hampshire and the Contractor hereby mutually agree as follows:

GENERAL PROVISIONS**1. IDENTIFICATION.**

1.1 State Agency Name The Department of Health and Human Services		1.2 State Agency Address 129 Pleasant Street Concord, NH 03301-3857	
1.3 Contractor Name FDGS, Limited Partnership, a/k/a First Data Government Solutions, Limited Partnership		1.4 Contractor Address 255 FiServ Dr., Brookfield, WI, 53045	
1.5 Contractor Phone Number 262-879-5000	1.6 Account Number 05-95-48-480030-9318-034-5000 99 / 05-95-47-470010-8009-102-500731	1.7 Completion Date June 30, 2026	1.8 Price Limitation \$1,700,000
1.9 Contracting Officer for State Agency Nathan D. White, Director		1.10 State Agency Telephone Number (603) 271-9637	
1.11 Contractor Signature <div style="display: flex; justify-content: space-between; align-items: center;"> <div>Date: 9/2/2022</div> </div>		1.12 Name and Title of Contractor Signatory Shane McCullough Authorized Signer	
1.13 State Agency Signature <div style="display: flex; justify-content: space-between; align-items: center;"> <div>Date: 9/2/2022</div> </div>		1.14 Name and Title of State Agency Signatory Melissa Hardy Director, DLTSS	
1.15 Approval by the N.H. Department of Administration, Division of Personnel (if applicable) <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div>By:</div> <div>Director, On:</div> </div>			
1.16 Approval by the Attorney General (Form, Substance and Execution) (if applicable) <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div>By: </div> <div>Attorney On: 9/4/2022</div> </div>			
1.17 Approval by the Governor and Executive Council (if applicable) <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div>G&C Item number:</div> <div>G&C Meeting Date:</div> </div>			

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
STATE OF NEW HAMPSHIRE GENERAL PROVISIONS - P37

2. SERVICES TO BE PERFORMED. The State of New Hampshire, acting through the agency identified in block 1.1 ("State"), engages contractor identified in block 1.3 ("Contractor") to perform, and the Contractor shall perform, the work or sale of goods, or both, identified and more particularly described in the attached EXHIBIT B which is incorporated herein by reference ("Services").

3. EFFECTIVE DATE/COMPLETION OF SERVICES.

3.1 Notwithstanding any provision of this Agreement to the contrary, and subject to the approval of the Governor and Executive Council of the State of New Hampshire, if applicable, this Agreement, and all obligations of the parties hereunder, shall become effective on the date the Governor and Executive Council approve this Agreement as indicated in block 1.17, unless no such approval is required, in which case the Agreement shall become effective on the date the Agreement is signed by the State Agency as shown in block 1.13 ("Effective Date").

3.2 If the Contractor commences the Services prior to the Effective Date, all Services performed by the Contractor prior to the Effective Date shall be performed at the sole risk of the Contractor, and in the event that this Agreement does not become effective, the State shall have no liability to the Contractor, including without limitation, any obligation to pay the Contractor for any costs incurred or Services performed. Contractor must complete all Services by the Completion Date specified in block 1.7.

4. CONDITIONAL NATURE OF AGREEMENT.

Notwithstanding any provision of this Agreement to the contrary, all obligations of the State hereunder, including, without limitation, the continuance of payments hereunder, are contingent upon the availability and continued appropriation of funds affected by any state or federal legislative or executive action that reduces, eliminates or otherwise modifies the appropriation or availability of funding for this Agreement and the Scope for Services provided in EXHIBIT B, in whole or in part. In no event shall the State be liable for any payments hereunder in excess of such available appropriated funds. In the event of a reduction or termination of appropriated funds, the State shall have the right to withhold payment until such funds become available, if ever, and shall have the right to reduce or terminate the Services under this Agreement immediately upon giving the Contractor notice of such reduction or termination. The State shall not be required to transfer funds from any other account or source to the Account identified in block 1.6 in the event funds in that Account are reduced or unavailable.

5. CONTRACT PRICE/PRICE LIMITATION/ PAYMENT.

5.1 The contract price, method of payment, and terms of payment are identified and more particularly described in EXHIBIT C which is incorporated herein by reference.

5.2 The payment by the State of the contract price shall be the only and the complete reimbursement to the Contractor for all expenses, of whatever nature incurred by the Contractor in the performance hereof, and shall be the only and the complete compensation to the Contractor for the Services. The State shall have no liability to the Contractor other than the contract price.

5.3 The State reserves the right to offset from any amounts otherwise payable to the Contractor under this Agreement those liquidated amounts required or permitted by N.H. RSA 80:7 through RSA 80:7-c or any other provision of law.

5.4 Notwithstanding any provision in this Agreement to the contrary, and notwithstanding unexpected circumstances, in no event shall the total of all payments authorized, or actually made hereunder, exceed the Price Limitation set forth in block 1.8.

6. COMPLIANCE BY CONTRACTOR WITH LAWS AND REGULATIONS/ EQUAL EMPLOYMENT OPPORTUNITY.

6.1 In connection with the performance of the Services, the Contractor shall comply with all applicable statutes, laws, regulations, and orders of federal, state, county or municipal authorities which impose any obligation or duty upon the Contractor, including, but not limited to, civil rights and equal employment opportunity laws. In addition, if this Agreement is funded in any part by monies of the United States, the Contractor shall comply with all federal executive orders, rules, regulations and statutes, and with any rules, regulations and guidelines as the State or the United States issue to implement these regulations. The Contractor shall also comply with all applicable intellectual property laws.

6.2 During the term of this Agreement, the Contractor shall not discriminate against employees or applicants for employment because of race, color, religion, creed, age, sex, handicap, sexual orientation, or national origin and will take affirmative action to prevent such discrimination.

6.3. The Contractor agrees to permit the State or United States access to any of the Contractor's books, records and accounts for the purpose of ascertaining compliance with all rules, regulations and orders, and the covenants, terms and conditions of this Agreement.

7. PERSONNEL.

7.1 The Contractor shall at its own expense provide all personnel necessary to perform the Services. The Contractor warrants that all personnel engaged in the Services shall be qualified to perform the Services, and shall be properly licensed and otherwise authorized to do so under all applicable laws.

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
STATE OF NEW HAMPSHIRE GENERAL PROVISIONS - P37

7.2 Unless otherwise authorized in writing, during the term of this Agreement, and for a period of six (6) months after the Completion Date in block 1.7, the Contractor shall not hire, and shall not permit any subcontractor or other person, firm or corporation with whom it is engaged in a combined effort to perform the Services to hire, any person who is a State employee or official, who is materially involved in the procurement, administration or performance of this Agreement. This provision shall survive termination of this Agreement.

7.3 The Contracting Officer specified in block 1.9, or his or her successor, shall be the State's representative. In the event of any dispute concerning the interpretation of this Agreement, the Contracting Officer's decision shall be final for the State.

8. EVENT OF DEFAULT/REMEDIES.

8.1 Any one or more of the following acts or omissions of the Contractor shall constitute an event of default hereunder ("Event of Default"):

- 8.1.1 failure to perform the Services satisfactorily or on schedule;
- 8.1.2 failure to submit any report required hereunder; and/or
- 8.1.3 failure to perform any other covenant, term or condition of this Agreement.

8.2 Upon the occurrence of any Event of Default, the State may take any one, or more, or all, of the following actions:

8.2.1 give the Contractor a written notice specifying the Event of Default and requiring it to be remedied within, in the absence of a greater or lesser specification of time, thirty (30) days from the date of the notice; and if the Event of Default is not timely cured, terminate this Agreement, effective two (2) days after giving the Contractor notice of termination;

8.2.2 give the Contractor a written notice specifying the Event of Default and suspending all payments to be made under this Agreement and ordering that the portion of the contract price which would otherwise accrue to the Contractor during the period from the date of such notice until such time as the State determines that the Contractor has cured the Event of Default shall never be paid to the Contractor;

8.2.3 give the Contractor a written notice specifying the Event of Default and set off against any other obligations the State may owe to the Contractor any damages the State suffers by reason of any Event of Default; and/or

8.2.4 give the Contractor a written notice specifying the Event of Default, treat the Agreement as breached, terminate the Agreement and pursue any of its remedies at law or in equity, or both.

8.3. No failure by the State to enforce any provisions hereof after any Event of Default shall be deemed a waiver of its rights with regard to that Event of Default, or any subsequent Event of Default. No express failure to enforce any Event of Default shall be deemed a waiver of the right of the State to enforce each and all of the provisions hereof upon any further or other Event of Default on the part of the Contractor.

9. TERMINATION.

9.1 Notwithstanding paragraph 8, the State may, at its sole discretion, terminate the Agreement for any reason, in whole or in part, by thirty (30) days written notice to the Contractor that the State is exercising its option to terminate the Agreement.

9.2 In the event of an early termination of this Agreement for any reason other than the completion of the Services, the Contractor shall, at the State's discretion, deliver to the Contracting Officer, not later than fifteen (15) days after the date of termination, a report ("Termination Report") describing in detail all Services performed, and the contract price earned, to and including the date of termination. The form, subject matter, content, and number of copies of the Termination Report shall be identical to those of any Final Report described in the attached EXHIBIT B. In addition, at the State's discretion, the Contractor shall, within 15 days of notice of early termination, develop and submit to the State a Transition Plan for services under the Agreement.

10. DATA/ACCESS/CONFIDENTIALITY/PRESERVATION.

10.1 As used in this Agreement, the word "data" shall mean all information and things developed or obtained during the performance of, or acquired or developed by reason of, this Agreement, including, but not limited to, all studies, reports, files, formulae, surveys, maps, charts, sound recordings, video recordings, pictorial reproductions, drawings, analyses, graphic representations, computer programs, computer printouts, notes, letters, memoranda, papers, and documents, all whether finished or unfinished.

10.2 All data and any property which has been received from the State or purchased with funds provided for that purpose under this Agreement, shall be the property of the State, and shall be returned to the State upon demand or upon termination of this Agreement for any reason.

10.3 Confidentiality of data shall be governed by N.H. RSA chapter 91-A or other existing law. Disclosure of data requires prior written approval of the State.

11. CONTRACTOR'S RELATION TO THE STATE. In the performance of this Agreement the Contractor is in all respects an independent contractor, and is neither an agent nor an employee of the State. Neither the Contractor nor any of its officers, employees, agents or members shall have authority to bind the State or receive any benefits, workers' compensation or other emoluments provided by the State to its employees.

12. ASSIGNMENT/DELEGATION/SUBCONTRACTS.

12.1 The Contractor shall not assign, or otherwise transfer any interest in this Agreement without the prior written notice, which shall be provided to the State at least fifteen (15) days prior to the

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
STATE OF NEW HAMPSHIRE GENERAL PROVISIONS - P37

assignment, and a written consent of the State. For purposes of this paragraph, a Change of Control shall constitute assignment. "Change of Control" means (a) merger, consolidation, or a transaction or series of related transactions in which a third party, together with its affiliates, becomes the direct or indirect owner of fifty percent (50%) or more of the voting shares or similar equity interests, or combined voting power of the Contractor, or (b) the sale of all or substantially all of the assets of the Contractor.

12.2 None of the Services shall be subcontracted by the Contractor without prior written notice and consent of the State. The State is entitled to copies of all subcontracts and assignment agreements and shall not be bound by any provisions contained in a subcontract or an assignment agreement to which it is not a party.

13. INDEMNIFICATION. Unless otherwise exempted by law, the Contractor shall indemnify and hold harmless the State, its officers and employees, from and against any and all claims, liabilities and costs for any personal injury or property damages, patent or copyright infringement, or other claims asserted against the State, its officers or employees, which arise out of (or which may be claimed to arise out of) the acts or omission of the Contractor, or subcontractors, including but not limited to the negligence, reckless or intentional conduct. The State shall not be liable for any costs incurred by the Contractor arising under this paragraph 13. Notwithstanding the foregoing, nothing herein contained shall be deemed to constitute a waiver of the sovereign immunity of the State, which immunity is hereby reserved to the State. This covenant in paragraph 13 shall survive the termination of this Agreement.

14. INSURANCE.

14.1 The Contractor shall, at its sole expense, obtain and continuously maintain in force, and shall require any subcontractor or assignee to obtain and maintain in force, the following insurance:

14.1.1 commercial general liability insurance against all claims of bodily injury, death or property damage, in amounts of not less than \$1,000,000 per occurrence and \$2,000,000 aggregate or excess; and

14.1.2 special cause of loss coverage form covering all property subject to subparagraph 10.2 herein, in an amount not less than 80% of the whole replacement value of the property.

14.2 The policies described in subparagraph 14.1 herein shall be on policy forms and endorsements approved for use in the State of New Hampshire by the N.H. Department of Insurance, and issued by insurers licensed in the State of New Hampshire.

14.3 The Contractor shall furnish to the Contracting Officer identified in block 1.9, or his or her successor, a certificate(s) of insurance for all insurance required under this Agreement. Contractor shall also furnish to the Contracting Officer identified in block 1.9, or his or her successor, certificate(s) of insurance for

all renewal(s) of insurance required under this Agreement no later than ten (10) days prior to the expiration date of each insurance policy. The certificate(s) of insurance and any renewals thereof shall be attached and are incorporated herein by reference.

15. WORKERS' COMPENSATION.

15.1 By signing this agreement, the Contractor agrees, certifies and warrants that the Contractor is in compliance with or exempt from, the requirements of N.H. RSA chapter 281-A ("*Workers' Compensation*").

15.2 To the extent the Contractor is subject to the requirements of N.H. RSA chapter 281-A, Contractor shall maintain, and require any subcontractor or assignee to secure and maintain, payment of Workers' Compensation in connection with activities which the person proposes to undertake pursuant to this Agreement. The Contractor shall furnish the Contracting Officer identified in block 1.9, or his or her successor, proof of Workers' Compensation in the manner described in N.H. RSA chapter 281-A and any applicable renewal(s) thereof, which shall be attached and are incorporated herein by reference. The State shall not be responsible for payment of any Workers' Compensation premiums or for any other claim or benefit for Contractor, or any subcontractor or employee of Contractor, which might arise under applicable State of New Hampshire Workers' Compensation laws in connection with the performance of the Services under this Agreement.

16. NOTICE. Any notice by a party hereto to the other party shall be deemed to have been duly delivered or given at the time of mailing by certified mail, postage prepaid, in a United States Post Office addressed to the parties at the addresses given in blocks 1.2 and 1.4, herein.

17. AMENDMENT. This Agreement may be amended, waived or discharged only by an instrument in writing signed by the parties hereto and only after approval of such amendment, waiver or discharge by the Governor and Executive Council of the State of New Hampshire unless no such approval is required under the circumstances pursuant to State law, rule or policy.

18. CHOICE OF LAW AND FORUM. This Agreement shall be governed, interpreted and construed in accordance with the laws of the State of New Hampshire, and is binding upon and inures to the benefit of the parties and their respective successors and assigns. The wording used in this Agreement is the wording chosen by the parties to express their mutual intent, and no rule of construction shall be applied against or in favor of any party. Any actions arising out of this Agreement shall be brought and maintained in New Hampshire Superior Court which shall have exclusive jurisdiction thereof.

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
STATE OF NEW HAMPSHIRE GENERAL PROVISIONS - P37

19. CONFLICTING TERMS. In the event of a conflict between the terms of this P-37 form (as modified in EXHIBIT A) and/or attachments and amendment thereof, the terms of the P-37 (as modified in EXHIBIT A) shall control.

20. THIRD PARTIES. The parties hereto do not intend to benefit any third parties and this Agreement shall not be construed to confer any such benefit.

21. HEADINGS. The headings throughout the Agreement are for reference purposes only, and the words contained therein shall in no way be held to explain, modify, amplify or aid in the interpretation, construction or meaning of the provisions of this Agreement.

22. SPECIAL PROVISIONS. Additional or modifying provisions set forth in the attached EXHIBIT A are incorporated herein by reference.

23. SEVERABILITY. In the event any of the provisions of this Agreement are held by a court of competent jurisdiction to be contrary to any state or federal law, the remaining provisions of this Agreement will remain in full force and effect.

24. ENTIRE AGREEMENT. This Agreement, which may be executed in a number of counterparts, each of which shall be deemed an original, constitutes the entire agreement and understanding between the parties, and supersedes all prior agreements and understandings with respect to the subject matter hereof.

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT A – SPECIAL PROVISIONS

EXHIBIT A - SPECIAL PROVISIONS

The terms outlined in the P-37 General Provisions are modified as set forth below:

A.1 Provision 3, Effective Date/Completion of Services, is updated with the following addition:

3.3 The Term may be extended up to four (4) years, ("Extended Term") at the sole option of the State, subject to the parties prior written Agreement on applicable fees for each extended Term, up to but not beyond June 30, 2030 under the same terms and conditions, subject to approval of the Governor and Executive Council.

A.2 Provision 5, Contract Price/Price Limitation/ Payment, is updated with the following addition:

5.5 The State's liability under this Agreement shall be limited to monetary damages not to exceed the contract price pursuant to Paragraph 5.2. The Contractor agrees that it has an adequate remedy at law for any breach of this Agreement by the State and hereby waives any right to specific performance or other equitable remedies against the State. Subject to applicable laws and regulations, in no event shall the State be liable for any consequential, special, indirect, incidental, punitive, or exemplary damages. Notwithstanding the foregoing, nothing herein contained shall be deemed to constitute a waiver of the sovereign immunity of the State, which immunity is hereby reserved to the State.

A.3 Provision 8, Event of Default/Remedies, is updated with the following addition:

8.2.5 Give the Contractor a written notice specifying the event of Default, terminate the agreement as breached, and procure Services that are the subject of the Contract from another source and Contractor shall be liable for reimbursing the State for the replacement Services, and all administrative costs directly related to the replacement of the Contract and procuring the Services from another source, such as costs of competitive bidding, mailing, advertising, applicable fees, charges or penalties, and staff time costs; all of which shall be subject to the limitations of liability set forth in the Contract.

A.4 Provision 9, Termination, is deleted and replaced with the following:

9. TERMINATION

9.1 Notwithstanding paragraph 8, the State may, at its sole discretion, and with written notice, terminate the Agreement for any reason, in whole or in part. In the event of such termination, the Contractor shall immediately stop all work hereunder and shall immediately cause any and all of its suppliers and subcontractors to cease work. The State shall be liable for cost of all Services and Deliverables for which Acceptance has been given by the State, provided through the date of termination but will not be liable for any costs for incomplete Services or winding down the Contract activities. The Contractor shall not be paid for any work performed or costs incurred which reasonably could have been avoided.

**STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT A – SPECIAL PROVISIONS**

9.2 Termination Procedure

9.2.1 Upon termination of the Contract, the State, in addition to any other rights provided in the Contract, may require Contractor to deliver to the State any property, including without limitation, Software and Written Deliverables, for such part of the Contract as has been terminated.

9.2.2 After receipt of a notice of termination, and except as otherwise directed by the State, the Contractor shall:

- a. Stop work under the Contract on the date, and to the extent specified, in the notice;
- b. Promptly, but in no event longer than ten (10) days after termination, terminate its orders and subcontracts related to the work which has been terminated, and settle all outstanding liabilities and all claims arising out of such termination of orders and subcontracts, with the approval or ratification of the State to the extent required, which approval or ratification shall be final for the purpose of this Section;
- c. Take such action as the State directs, or as necessary to preserve and protect the property related to the Contract which is in the possession of Contractor and in which the State has an interest;
- d. Take no action to intentionally erase or destroy any State Data, which includes State Data held by the Contractor's subcontractors;
- e. Transfer title to the State and deliver in the manner, at the times, and to the extent directed by the State, any property which is required to be furnished to the State and which has been accepted or requested by the State;
- f. Work with the State to develop a Services and Data Transition Plan per the "Contract End-of-Life Transition" requirement in the Additional Requirements section of this Contract; and
- g. Provide written Certification to the State that Contractor has surrendered to the State all said property.

9.2.3 If the Contract has expired, or terminated prior to the Completion Date, for any reason, the Contractor shall provide, for a period up to ninety (90) days after the expiration or termination, all transition services requested by the State, at no additional cost, to allow for the expired or terminated portion of the Services to continue without interruption or adverse effect, and to facilitate the orderly transfer of such Services to the State or its designees ("Transition Services").

9.2.4 This covenant in paragraph 9 shall survive the termination of this Contract.

A.5 Provision 10, Data/Access/Confidentiality/Preservation, is updated with the following addition:

10.4 In performing its obligations under this Agreement, Contractor may gain access to Confidential Information of the State. Confidential Information is defined in the Department of Health and Human Services' Information Security Requirements in Exhibit G, Attachments and Contractor Exhibits, Section 1, Attachments,

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT A – SPECIAL PROVISIONS

Subsection b., DHHS Agency Compliance Documents – Attachment 2, Exhibit K, DHHS Information Security Requirements.

10.5 Subject to applicable federal or State laws and regulations, Confidential Information shall not include information which:

- a. shall have otherwise become publicly available other than as a result of disclosure by the receiving Party in breach hereof;
- b. was disclosed to the receiving Party on a non-confidential basis from a source other than the disclosing Party, which the receiving Party believes is not prohibited from disclosing such information as a result of an obligation in favor of the disclosing Party; or
- c. is disclosed with the written consent of the disclosing Party's Privacy Officer or designee.

10.6 Contractor Confidential Information. Contractor shall clearly identify in writing all information it claims to be confidential or proprietary upon providing such information to the State. For the purposes of complying with its legal obligations, the State is under no obligation to accept the Contractor's designation of material as confidential. Contractor acknowledges that the State is subject to State and federal laws governing disclosure of information including, but not limited to, RSA Chapter 91-A. In the event the State receives a request for the information identified by Contractor as confidential or proprietary, the State shall notify Contractor and specify the date the State will be releasing the requested information. At the request of the State, Contractor shall cooperate and assist the State with the collection and review of Contractor's information, at no additional expense to the State. Any effort to prohibit or enjoin the release of the information shall be Contractor's sole responsibility and at Contractor's sole expense. If Contractor fails to obtain a court order enjoining the disclosure, the State shall release the information on the date specified in the State's notice to Contractor, without any liability to the State.

10.7 This covenant in paragraph 10 shall survive the termination of this Contract.

A.6 Provision 12, Assignment/Delegation/Subcontracts, is updated with the following addition:

12.3 Subcontractors are subject to the same contractual conditions as the Contractor and the Contractor is responsible to ensure subcontractor compliance with those conditions. The Contractor shall have written agreements with all subcontractors, specifying the work to be performed, and if applicable, a Business Associate Agreement in accordance with the Health Insurance Portability and Accountability Act. Written agreements shall specify how corrective action shall be managed. The Contractor shall manage the subcontractor's performance on an ongoing basis and take corrective action as necessary. The Contractor shall annually provide the State with a list of all subcontractors provided for under this Agreement and notify the State of any inadequate subcontractor performance. Failure to enter into business associate agreements with its subcontractors that create or receive PHI on the behalf of DHHS through this Contract, and failure to comply with the implementation specifications for such agreements is a direct HIPAA violation by the Contractor.

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT A – SPECIAL PROVISIONS

12.4 In the event that Contractor should change ownership for any reason whatsoever that results in a change of control of the Contractor, the State shall have the option of:

- a. continuing under the Agreement with Contractor, its successors or assigns for the full remaining Term of the Agreement or for such period of time as determined necessary by the State; or
- b. immediately terminate the Agreement without liability to or further compensation owed to Contractor, its successors or assigns.

A.7 The following Provisions are added and made part of the P37:

25. FORCE MAJEURE

25.1 Neither Contractor nor the State shall be responsible for delays or failures in performance resulting from events beyond the control of such Party and without fault or negligence of such Party. Such events shall include, but not be limited to, acts of God, strikes, lockouts, riots, and acts of War, epidemics, pandemics, acts of Government, fire, power failures, nuclear accidents, earthquakes, and unusually severe weather.

25.2 Except in the event of the foregoing, Force Majeure events shall not include the Contractor's inability to hire or provide personnel needed for the Contractor's performance under the Contract.

26. EXHIBITS/ATTACHMENTS

The Exhibits and Attachments referred to in and attached to the Contract are incorporated by reference herein, including the Department of Health and Human Services Exhibits D-K referenced in Exhibit G of this Agreement

27. NON-EXCLUSIVE CONTRACT

The State reserves the right, at its discretion, to retain other Contractors to provide any of the Services or Deliverables identified under this Agreement. Contractor shall make best efforts to coordinate work with all other State Contractors performing Services that relate to the work or Deliverables set forth in the Agreement. The State intends to use, whenever possible, existing Software and hardware contracts to acquire supporting Software and hardware.

28. GOVERNMENT APPROVALS

Contractor shall obtain all necessary and applicable regulatory or other governmental approvals necessary to perform its obligations under the Contract.

29. ORDER OF PRECEDENCE

In the event of conflict or ambiguity among any of the text within this agreement, the following Order of Precedence shall govern:

- i. State of New Hampshire, Department of Health and Human Services Contract Agreement RFP-2022-DLTSS-05-ELECT -01- 2022-031.

**STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT A – SPECIAL PROVISIONS**

- ii. State of New Hampshire, Department of Health and Human Services Request for Proposals RFP-2022-DLTSS-05-ELECT Electronic Visit Verification System.
- iii. Contractor Proposal Response to Department of Health and Human Services RFP-2022-DLTSS-05-ELECT Electronic Visit Verification System dated March 8, 2022.

Remainder of this page intentionally left blank

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHINCAL REQUIREMENTS AND DELIVERABLES

EXHIBIT B – STATEMENT OF WORK (SOW) BUSINESS AND TECHNICAL REQUIREMENTS AND DELIVERABLES

The Statement of Work, Business and Technical Requirements, and Deliverables are set forth below:

1. STATEMENT OF WORK

1.1. Concept of Operations

- 1.1.1. The Contractor shall provide the proprietary AuthentiCare® solution (Authenticare EVV System) as a single, integrated platform with both electronic visit verification (EVV) data collection and data aggregator components, to be used by the Department and the Department's providers for the services listed on Chart 1.1.5 below.
- 1.1.2. The Department reserves the right to make modifications to Chart 1.1.5 as new services are added or existing services are removed to meet the needs of the Department.
- 1.1.3. Procedure and billing code modifiers in Chart 1.1.5, Columns Medicaid Management Information System (MMIS) Mod1, MMIS Mod2 and MMIS Mod3, below, identify the specific services that will require EVV. MMIS billing code modifiers are:
- 1.1.3.1. Choices for Independence, 1915(c) Home and Community Based Service Waiver; (HC – CFI) Waiver
- 1.1.3.2. SE – Acquired Brain Disorder, (ABD), Developmental Disabilities (DD) or In Home Support Waiver for Children with Developmental Disabilities (his) Waiver
- 1.1.3.3. UA – DD Waiver
- 1.1.3.4. UB – ABD Waiver
- 1.1.3.5. UC – IHS Waiver
- 1.1.3.6. U1-U8 – Differentiates the service

Table B-1						
EVV Phase	Program/ Waiver	Service Description	MMIS Procedure Code	MMIS Claims Billing Modifier 1 (Mod1)	MMIS Claims Billing Modifier 2 (Mod2)	MMIS Claims Billing Modifier 3 (Mod3)
Personal Care	CFI	Participant Directed Services Personal Care	T1019	HC	U3	
Personal Care	CFI	Personal Care Agency Directed	T1019	HC	U1	

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHINICAL REQUIREMENTS AND DELIVERABLES

Table B-1						
EVV Phase	Program/ Waiver	Service Description	MMIS Procedure Code	MMIS Claims Billing Modifier 1 (Mod1)	MMIS Claims Billing Modifier 2 (Mod2)	MMIS Claims Billing Modifier 3 (Mod3)
Personal Care	CFI	Personal Care Consumer Directed	T1019	HC	U2	
Personal Care	CFI	Personal Care Special Rate	T1019	HC	U4	
Personal Care	IHS	Participant Directed & Managed Personal Care	T2025	SE	UC	U1
Personal Care	State Plan	Personal Care Attendant Services	T1019			
Home Health	ABD	ABD Consumer Directed Services — Family Support/Respite**	T2025	SE	UB	U5
Home Health	ABD	ABD Respite Medical/Behavioral* *	T1005	SE	UB	U2
Home Health	ABD	ABD Respite**	T1005	SE	UB	U1
Home Health	CFI	Home Health Aide 8+ Units	G0156	HC	U1	
Home Health	CFI	Home Health Aide Per Visit	T1021	HC		
Home Health	CFI	Respite Care Services**	T1005	HC		
Home Health	CFI	Respite Care Special Rates**	T1005	HC	U1	
Home Health	CFI	Skilled Nurse Per Visit	T1030	HC		
Home Health	DD	Consumer Directed Services - Family Support/Respite**	T2025	SE	UA	U5
Home Health	DD	Respite Behavioral/Medical* *	T1005	SE	UA	U2
Home Health	DD	Respite**	T1005	SE	UA	U1
Home Health	IHS	Participant Directed & Managed Respite**	T2025	SE	UC	U4
Home Health	State Plan	Home Health Aide 8+ Units	G0156			

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHNICAL REQUIREMENTS AND DELIVERABLES

Table B-1						
EVV Phase	Program/ Waiver	Service Description	MMIS Procedure Code	MMIS Claims Billing Modifier 1 (Mod1)	MMIS Claims Billing Modifier 2 (Mod2)	MMIS Claims Billing Modifier 3 (Mod3)
Home Health	State Plan	Home Health Aide Per Visit	T1021			
Home Health	State Plan	Occupational Therapy**	G0152			
Home Health	State Plan	Physical Therapy**	G0151			
Home Health	State Plan	Private Duty LPN (State Plan)	S9124			
Home Health	State Plan	Private Duty RN (State Plan)	S9123			
Home Health	State Plan	Skilled Nurse Per Visit	T1030			
Home Health	State Plan	Speech Therapy**	G0153			

** When provided in the home

2. PROJECT STAKEHOLDERS

- 2.1. At a minimum, the following stakeholders must be engaged during the project to provide input for the Authenticare EVV System:

Table B-2		
State Staff:		
Organization	Title	Role
DLTSS	Director	Executive Management
BDS	Bureau Chief	Management
BDS	Program Specialist	Pre-authorization SME
BEAS	Bureau Chief	Management
BEAS	Administrator	Pre-authorization SME
Division of Medicaid Services	Medicaid Director	Executive Management
Division of Medicaid Services	Medical Services Administrator	Medical Management SME
Division of Medicaid Services	Administrator	Managed Care SME
Program Quality and Integrity	Program Integrity Administrator	Program Integrity SME
Office of Information Services	Director of Information Services	Executive Management
Office of Information Services	Deputy Information Security Officer Information Technology Manager V	Department Information Security
Office of Information Services	Information Technology Manager IV	Enterprise Business Intelligence Manager

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHNICAL REQUIREMENTS AND DELIVERABLES

Table B-2		
MES Core Team	Information Technology Manager	Co-Project Manager
MES Core Team	Information Technology Manager	Medicaid Management Information System (MMIS)
Consulting Services	Information Technology Manager	Co-Project Manager
DoIT	Information Technology Manager	Medicaid Management Information System (MMIS)
DoIT	Information Technology Manager	IT Leader for DHHS
EVV Advisory Council Members:		
Organization	Title	Roles
Community Providers (Multiple)	Executive Director, Business Manager, IT	Community Personal Care and Home Health Care Provider SMEs
Community Services Network, Inc. (CSNI)	Director of Information Services	Developmental Services Area Agency SME
Granite State Independent Living (GSIL)	Chief Executive Officer	Statewide Independent Living Center SME
GSIL Consumer Advisory Council	Consumer	Self-Advocacy SME
Home Care, Hospice and Palliative Care Alliance of New Hampshire	Chief Executive Officer	Home Health SME
Managed Care Organizations	IT Directors / EVV Product Owners	Managed Care SME
NH State Family Support Council	Chairperson	Family Self-Advocacy SME

3. SCOPE OF SERVICES

3.1. The Contractor shall ensure the Authenticare EVV System:

- 3.1.1. Ensures individuals receive the services that they are authorized to receive in order to stay healthy and safe in the community;
- 3.1.2. Complies with the requirements within the 21st Century Cures Act and is consistent with all applicable federal law;
- 3.1.3. Is developed through a collaborative stakeholder process;
- 3.1.4. Is developed in a manner that respects recipients and providers, does not alter their Olmstead protections and is minimally burdensome;
- 3.1.5. Does not change the number of service hours, nor how or where services are delivered;
- 3.1.6. Leverages the Department's existing and future information systems, and

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHNICAL REQUIREMENTS AND DELIVERABLES

- 3.1.7. Includes training for providers, recipients and other stakeholders in how to use the Authenticare EVV System, as approved by the Department.
- 3.1.8. Meet Cures Act requirements, including;
 - 3.1.8.1. Meeting CURES Act requirements for EVV to ensure compliance penalties from the Center for Medicaid Services (CMS) are mitigated and/or avoided; and
 - 3.1.8.2. With the CMS directed outcomes for EVV inherently addressing compliance, this outcome focuses on other compliance projects. The associated requirements for this outcome leverages compliance requirements approved by CMS for National Association of State Procurement Officers (NASPO) driven multi-state module implementations.
- 3.1.9. Monitors and prevents fraud, including:
 - 3.1.9.1. Providing the Department with enhanced ability to monitor and prevent fraud, waste and abuse through increased visibility into its State Plan and Home and Community-Based Services programs; and
 - 3.1.9.2. Capturing the location, date and time of service delivery, and automatically flags visits if key EVV data elements are missing or have been changed manually; and
 - 3.1.9.3. Subjecting every visit to a claim workflow that applies exceptions and prevents providers from billing for incomplete or unauthorized services.
- 3.1.10. Provides no less than two technology platforms to track time and location of direct care providers during service delivery , including;
 - 3.1.10.1. AuthentiCare Mobile App, that must:
 - 3.1.10.1.1. Comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA);
 - 3.1.10.1.2. Provide a secure connection to an AuthentiCare web service to record visit activity;
 - 3.1.10.1.3. Save visit information in real time when a connection to the internet or cellular network is available;
 - 3.1.10.1.4. Capture visit data offline when there is no Wi-Fi or cellular data coverage at the time and location of service delivery and:
 - 3.1.10.1.4.1. Encrypt and store the visit data on the device until a connection is restored; and
 - 3.1.10.1.4.2. Forward visit details to the AuthentiCare servers when a connection is restored (Store and Forward);

**STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHNICAL REQUIREMENTS AND DELIVERABLES**

- 3.1.10.2. AuthentiCare's Interactive Voice Response (IVR) system that can be used with any standard land line, cable service phone, or other phone service that is tied to the client's home or other location approved for service delivery;
- 3.1.11. Is reliable, accessible, and minimally burdensome on providers, members, and their caregivers.
- 3.2. The Contractor shall ensure the following features of the Authenticare EVV system are optimized to meet the needs of the Department and that the cost of ownership is optimized for:
 - 3.2.1. Delivery;
 - 3.2.2. Implementation;
 - 3.2.3. Operations;
 - 3.2.4. Maintenance;
 - 3.2.5. Upgrades and Device Management;
 - 3.2.6. Change Management;
 - 3.2.7. Service Level Agreement (SLA);
 - 3.2.8. Alignment to Industry Standards, and the State's future system integration and/or Enterprise Service Bus, for Interfaces and other upcoming Standards; and
 - 3.2.9. Training.
- 3.3. The Contractor shall ensure high levels of satisfaction from all stakeholders regarding the ability to provide input and feedback into the design of the Authenticare EVV System for the Department, as measured by the outcome of improved satisfaction for stakeholders through stakeholder feedback and surveys. Stakeholders include, but are not limited to:
 - 3.3.1. Members.
 - 3.3.2. Family Member Caregivers.
 - 3.3.3. Direct Care Workers (Provider).
 - 3.3.4. The Department and other State agencies.
 - 3.3.5. Managed Care Organizations.
 - 3.3.6. Community Stakeholders.
- 3.4. The Contractor shall ensure the Authenticare EVV System maintains high levels of data quality and reliability to support timely and accurate processing and reporting, including multiple dashboards for specific roles that present real-time monitoring information to providers and administrative staff.
- 3.5. The Contractor shall ensure EVV data is readily portable to the Departments Enterprise Business Intelligence (EBI) platform using a direct connect of a State defined tool, such as Informatica

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHNICAL REQUIREMENTS AND DELIVERABLES

or Tableau to the source database via a service account or the exchange of flat files using Secure File Transfer Protocol, or other, State approved, secure means.

- 3.6. The Contractor shall ensure the Authenticare EVV System provides the following EVV scheduling, billing, and compliance capability and features:
- 3.6.1. Audited visit verification that prevents provider abuse or inappropriate billing/payment by collecting recipient and direct service worker information electronically at the beginning and end of services provided in the home and other settings;
 - 3.6.2. The ability to audit provider EVV systems to ensure compliance with CURES Act requirements;
 - 3.6.3. Monitoring and reporting for key performance indicators, to be determined by the Department;
 - 3.6.4. Claims Filing Related Services, including, but not limited to:
 - 3.6.4.1. Aggregator functionality to verify visits against billed claims and authorizations before processing for payment by the MMIS or MCOs.
 - 3.6.4.2. An 837 Electronic Data Interchange (EDI) claim submission process that groups claim transactions by payer into American National Standards Institute (ANSI) function groups.
 - 3.6.5. Reporting capability for key performance indicators that allows the Department to use data elements to query and generate ad-hoc reports, and that can provide a standard suite of reports to:
 - 3.6.5.1. The Department;
 - 3.6.5.2. Case management and area agencies;
 - 3.6.5.3. Members;
 - 3.6.5.4. Provider agencies; and
 - 3.6.5.5. Managed care organizations (MCO).
 - 3.6.6. Interfaces to and from the MMIS and provider systems that conform Medicaid Information Technology Architecture (MITA) standards that include, but are not limited to:
 - 3.6.6.1. Batch file processes
 - 3.6.6.2. Industry-standard specification (JSON/REST) web service transactions.
 - 3.6.6.3. Standard Application Programmer Interface (APIs) hosted by the Contractor.
 - 3.6.6.4. The ability to securely transfer data to the Authenticare system via the Authenticare website, SFTP or web services.

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHNICAL REQUIREMENTS AND DELIVERABLES

- 3.6.6.5. The ability to process multiple, concurrent file transfers where files of different types are received and generated at varying intervals.
- 3.6.6.6. HIPAA national standard X12 EDI transaction formats including, but not limited to 837/835, 276/277, 277CA, 270/271, 278 and 834 transaction formats.
- 3.6.6.7. Interfaces need to stay in synch with changes and updates to the MMIS architecture, software, and licensing needs.
- 3.6.7. Interfaces to and from the System Integration services to deliver and request data, reflecting the requirements enumerated in requirement 3.6.6 and all sub requirements.
- 3.6.8. Daily communication with the Department's MMIS to potentially exchange member, provider, service authorization, EVV visit, and claims information via an automated interface;
- 3.6.9. Ability to communicate with provider EVV systems and claims information, including certifying that external provider systems transmit all required data in the appropriate format.
- 3.6.10. Compliance with State and agency-specific information security and privacy requirements, including, but not limited to DHHS Agency Compliance Documents – Attachment 2, Exhibits I and K, including:
 - 3.6.10.1. A unique individual login for each system user.
 - 3.6.10.2. A defined role or roles for each system user.
 - 3.6.10.3. Full security and privacy review for each application release, including both static code scans and dynamic application scans.
 - 3.6.10.4. A reportable record of system access and activity, monthly or as requested.
 - 3.6.10.5. Online web reporting capability for of claim (visit) and authorization history.
- 3.7. The Contractor shall ensure the Authenticare EVV System provides for a variety of testing of all minor and major releases that incorporates quality assurance management processes and controls, which are documented in the overall testing processes, and based off industry best practices. Testing must include, but is not limited to:
 - 3.7.1. Privacy testing.
 - 3.7.2. User Acceptance Testing.
 - 3.7.3. System stress testing.
 - 3.7.4. Independent qualified third party security assessments and penetration testing.
 - 3.7.5. Disaster recovery methods testing.

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHNICAL REQUIREMENTS AND DELIVERABLES

- 3.8. The Contractor shall ensure Authenticare EVV System can monitor and report on KPIs/Metrics on an ongoing basis to support CMS certification requirements, as well as any KPIs/Metrics defined by the business for successful system usage.
- 3.9. The Contractor shall support the Department and the Department's contractor(s), if applicable, in Quality Assurance (QA) and Testing activities associated with the provision of EVV services, including, but not limited to:
 - 3.9.1. Providing requested information for Quality Assurance Requirements and Design Review.
 - 3.9.2. Participating in Operational Milestone Review(s).
- 3.10. The Contractor shall participate in CMS EVV Certification(s) Reviews.
- 3.11. The Contractor shall conduct an Operational Readiness Review (ORR) to validate all operations, including hardware, software, and telecommunications aspects of the Authenticare EVV System are ready for go-live.
- 3.12. The Contractor shall adhere to all Hosting and Cloud requirements.
- 3.13. The Contractor shall provide:
 - 3.13.1. Help desk support to end users with a Tier 1 Call Center accessible through email and telephone 8:00 a.m. to 8:00 p.m. Monday through Friday, Eastern Time, excluding holidays, and language line access when there is a need for language translation.
 - 3.13.2. Tier 2 Help Desk Specialists on call 24/7 to resolve or escalate issues that occur outside of standard business hours. and
 - 3.13.3. On-going system support and maintenance.
- 3.14. The Contractor shall assign a qualified full time project manager who will manage the project.
- 3.15. The Contract shall assign a CMS certification subject matter expert (SME) with knowledge of CMS Streamlined Modular Certification (SMC) processes, Medicaid Enterprise Systems, MITA standards and conditions and EVV solutions. The SME must:
 - 3.15.1. Review and stay current on CMS, HIPAA, NIST and other mandated requirements that may impact the scope, configuration and implementation of the Authenticare EVV System;
 - 3.15.2. Participate in design and delivery, providing guidance for keeping the project in line with certification requirements;
 - 3.15.3. Prepare for the Operational Readiness Review (ORR);
 - 3.15.4. Develop Key Performance Indicator (KPI)/Metrics reporting;
 - 3.15.5. Prepare for assembling the evidence package, including the live demonstration (if necessary) at the final ORR and Certification Review;
 - 3.15.6. Submit KPIs/Metrics and other artifacts and participate in the CMS final Certification Review;

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHNICAL REQUIREMENTS AND DELIVERABLES

- 3.15.7. Support State Medicaid Agency in completing any open items out of Certification Review;
- 3.15.8. Oversee CMS SMC approval and transition to Maintenance and Operations compliance activities;
- 3.15.9. Participate in project and technical meetings;
- 3.15.10. Review and approve reviews configuration design and development deliverables;
- 3.15.11. Ensure a repeatable process is created and executed by the Contractor to support the post certification operational reporting requirements of CMS.
- 3.15.12. Provide expert guidance and recommendations for addressing risks, issues, mitigations and changes that impact the state's certification and operational reporting; and
- 3.15.13. Work closely with state stakeholders toward the design and verification of the build-out during the DDI and Maintenance and Operations phases to ensure the Authenticare EVV System meets CMS certification criteria and state-specific requirements that include, but are not limited to:
 - 3.15.13.1. Security.
 - 3.15.13.2. Privacy.
 - 3.15.13.3. Data retention.
 - 3.15.13.4. CMS and federal requirements.
- 3.16. The Contractor shall develop a work plan in accordance with Exhibit G, EVV Business and Technical Requirements, Attachment 1, to be approved by the Department, that must include without limitation:
 - 3.16.1. A detailed description of the schedule;
 - 3.16.2. Tasks;
 - 3.16.3. Deliverables;
 - 3.16.4. Critical events;
 - 3.16.5. Task dependencies; and
 - 3.16.6. Payment Schedule.
- 3.17. The Contractor shall update the work plan no less than every two weeks, and review status and changes with the State's Project Manager.
 - 3.17.1. The Contractor will provide updates to the work plan and other project artifacts in the State's hosted Smartsheets environment.
- 3.18. Key Performance Measures and Liquidated Damages
 - 3.18.1. In the event the Contractor fails to meet the key performance measures specified within the Contract, the Department reserves the right to assess Liquidated Damages as described

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHNICAL REQUIREMENTS AND DELIVERABLES

below in Table 3.6.1, and in Appendix H, EVV Business and Technical Requirements. If assessed, the Liquidated Damages will be used to reduce the Department's payments to the Contractor or if the Liquidated Damages exceed amounts due from the Department, the Contractor will be required to make cash payments for the amount in excess. The Department may also delay the assessment of Liquidated Damages if it is in the best interest of the Department to do so. The Department may give notice to the Contractor of a failure to meet performance standards but delay the assessment of Liquidated Damages in order to give the Contractor an opportunity to remedy the deficiency. If the Contractor subsequently fails to remedy the deficiency to the satisfaction of the Department, the Department may reassert the assessment of Liquidated Damages, even following contract termination.

Table B-3		
Req. #	Key Performance Measure	Liquidated Damages
B12.1	The Contractor's solution shall be available twenty-four (24) hours a day, 7 days a week except for during scheduled maintenance. The Contractor shall ensure that the solution is available ninety-nine percent (99%) of the time as measured on a monthly basis and that downtime is no greater than twenty-four (24) hours per incident. Contractor shall provide five (5) workdays' notice to the State prior to its regularly scheduled maintenance windows. Availability is calculated monthly as follows: Availability percentage = unplanned downtime (Total downtime minus approved downtime) divided by Total time (24x7).	The Department will assess as specified below, per hour for each hour, or portion thereof, if the solution fails to meet the ninety-nine percent (99%) availability performance standard. \$1,000 per hour if zero (0) to twenty-four (24) hours beyond the availability performance standard. \$2,000 per hour if twenty-five (25) to forty-eight (48) hours beyond the availability performance standard. \$3,000 per hour if greater than forty-eight (48) hours beyond the availability performance standard.
B12.2	Provide real-time performance monitoring dashboard availability ninety-nine percent (99%) of the time, twenty-four (24) hours a day, seven (7) days a week, excluding Department approved planned downtime (i.e., system unavailable for use). Availability is calculated monthly as follows: Availability percentage = unplanned downtime (Total downtime minus approved downtime) divided by total time (24x7).	The Department will assess as specified below, per hour for each hour, or portion thereof, if the performance monitoring dashboard fails to meet the ninety-nine percent (99%) availability performance standard. \$500 per hour if zero (0) to twenty-four (24) hours beyond the availability performance standard. \$1,000 per hour if twenty-five (25) to forty-eight (48) hours beyond the availability performance standard.

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHNICAL REQUIREMENTS AND DELIVERABLES

Table B-3		
Req. #	Key Performance Measure	Liquidated Damages
		\$1,500 per hour if greater than forty-eight (48) hours beyond the availability performance standard.
B12.3	Request approval from the Department prior to scheduling non-emergency system downtime or maintenance during hours of operation no later than five (5) Business Days prior to downtime.	\$1,000 per occurrence if the request is not made by the specified deadline.
B12.4	Provide a user interface response time of less than two (2) seconds per discrete transaction. Response time is measured from the time the data packets leave the State network to the time a response is received from the Contractor's software application.	\$1,000 per month if the monthly average user interface response time is greater than two (2) seconds.
B12.5	The Contractor must ensure that the Data integrity error rate and routing errors of any transaction is less than .001%.	\$5,000 per month charge if the error rate exceeds one thousandths of a percent (0.001%) for the entire measured month for all transactions.
B12.6	Contractor shall replace key personnel within fifteen (15) State workdays. The State may grant additional time to replace key personnel if the Contractor makes interim arrangements to ensure that operations are not effected by loss of personnel.	\$500 per workday from 16th day of vacancy until filled with an employee approved by the Department.
B12.7	Request and receive written approval by the Department prior to releasing any public announcement concerning the Contract, including, but not limited to, notices, information pamphlets, press releases, research, reports, signs, and similar public notices prepared by or for the Contractor.	\$5,000 per public notice issued by the Contractor without pre-approval by the Department.
B12.8	All standardized reports shall be available online or delivered to authorized users by the scheduled time one hundred percent (100%) of the	\$500 per workday for each workday that each report is late, not distributed as required, or not in the approved format.

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHNICAL REQUIREMENTS AND DELIVERABLES

Table B-3		
Req. #	Key Performance Measure	Liquidated Damages
	time as defined and mutually agreed upon during detailed report design.	
B12.9	The Contractor must notify the State of any data load problems, discrepancies, or failures within one (1) workday of identification and present a resolution plan within three (3) workdays.	\$5,000 per workday for failure to meet the timeliness standard.
B12.10	The Contractor must have the capability to exchange and interface data with systems of record and process updates in near real time (within 3 seconds 99% of the time) transactions, excluding batch interface updates. Performance is measured by a predefined sample measuring the timestamp data was received to the timestamp the data is available to query in the database or presented to the user via a user interface.	\$2,000 per month if user accessibility based on the sample is greater than three seconds for more than one percent (1%) of the sample.
B12.11	The Contractor must receive data from third party/provider EVV systems and system of records (state systems) in near real time (within 3 seconds 99% of the time), excluding batch interface updates. Performance is measured by a predefined sample measuring the timestamp data was received to the timestamp the data is available to query in the database or presented to the user via a user interface.	\$2,000 per month if user accessibility based on the sample is greater than three seconds for more than one percent (1%) of the sample.
B12.12	The Contractor must demonstrate requirement compliance for one hundred percent (100%) of the requirements defined for each Department requested system modification by providing documentation such as system, integration, or parallel test results or demonstration of the specifications including Interfaces/APIs when	\$5,000 per modification implementation in which the Contractor is not able to demonstrate that one hundred percent (100%) of the requirements have been met by the Department-approved scheduled implementation date.

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHINCAL REQUIREMENTS AND DELIVERABLES

Table B-3		
Req. #	Key Performance Measure	Liquidated Damages
	requested. Compliance must be met by the Department approved implementation date.	
B12.13	The Contractor's help desk shall answer all calls within two (2) minutes or less of entering the queue, as determined based on the monthly average. The call abandonment rate shall be less than five percent (5%) as measured on a monthly basis.	\$1,000 per month if the monthly average call answer time is greater than two (2) minutes. \$1,000 per month if the monthly average call abandonment rate is greater than five percent (5%).
B12.14	The Contractor must respond to written, faxed, voicemail, or emailed inquiries within two (2) workdays of receipt.	\$1,000 per month if the monthly average response time is greater than two (2) workdays.
B12.15	The Contractor shall ensure all customer service interactions are logged in the Contractor's information systems with ninety-five percent (95%) of all issues resolved on the same day and one hundred percent (100%) of issues resolved within 30 calendar days.	\$2,000 per month if ninety-five percent (95%) of customer service interactions are not resolved within the same day. \$5,000 per month if one hundred percent (100%) of customer service interactions are not resolved within 30 calendar days.
B12.16	Class A Deficiencies/Defects - The Contractor shall have available to the State on-call telephone assistance, with issue tracking available to the State, eight (8) hours per day and five (5) days a week with an email / telephone response within two (2) hours of request; Class B & C Deficiencies/Defects – The State shall notify the Contractor of such Deficiencies/Defects during regular business hours and the Contractor shall respond back within four (4) hours of notification.	\$5,000 per deficiency if Class A deficiencies/defects are not responded to within two (2) hours during the workweek. \$2,000 per deficiency if Class B & C deficiencies/defects are not responded to within four (4) hours during the workweek.
B12.17	Provide the Contractor's plan for resolution within two (2) hours of the notification of the Class A deficiency to the Department and resolve the deficiency within twenty-four (24)	\$5,000 per 24-hour period past the two hours of notification and resolution within twenty-four (24) hours to seventy-two (72) hours.

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHNICAL REQUIREMENTS AND DELIVERABLES

Table B-3		
Req. #	Key Performance Measure	Liquidated Damages
	hours of the notification of the deficiency to the Department.	\$6,000 per 24-hour period from seventy-three (73) to one hundred sixty-eight (168) hours. \$7,000 per 24-hour period if more than one hundred sixty-eight (168) hours.
B12.18	Provide the Contractor's plan for resolution within four (4) hours of the notification of the Class B deficiency/defect to the Department and resolve the deficiency within thirty-six (36) hours of the notification of the deficiency to the Department.	\$3,000 per 24-hour period past the four hours of notification and resolution within thirty-six (36) hours to seventy-two (72) hours. \$2,000 per 24-hour period from seventy-three (73) to one hundred sixty-eight (168) hours. \$1,000 per 24-hour period if more than one hundred sixty-eight (168) hours.
B12.19	Produce and distribute new publications or amended publications in final form by the date requested by the Department.	\$100 per workday for each publication is not produced and distributed by the Department's requested due date.
B12.20	Maintain up to date functional documentation, including both user documentation and the Operations Procedure Manual.	\$100 per document, per workday the documentation does not match the functionality of the Contractor's solution.
B12.21	Training documentation shall be updated no more than ten (10) workdays after the implementation of a software change.	\$100 per Work Day beyond ten (10) workdays after the implementation of an applicable change.
B12.22	The Contractor shall make available all required reports in accordance with stated timeliness requirements.	\$100 charge per report for each workday after the report due date through the date the report is received or made available to the Department.
B12.23	The Contractor shall attend all meetings as required by the Department if advance notice is provided. The Department will stipulate whether in-person or remote/virtual attendance is required. Advance notice is defined as at least three (3) workdays prior to the meeting start time.	\$250 charge to the Contractor per occurrence.
B12.24	System change orders/requests shall be implemented by the mutually agreed upon due date.	\$500 per workday charge for orders/requests not completed by the due date.
B12.25	Restore availability within twenty-four (24) hours from the start of any	\$5,000 per 24-hour period starting from twenty-four (24) hours to seventy-two (72)

Page 28 of 72

Contractor Initials: SMDate: 9/2/2022

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHNICAL REQUIREMENTS AND DELIVERABLES

Table B-3		
Req. #	Key Performance Measure	Liquidated Damages
	disaster event involving the Contractor's solution, using procedures approved in the BCCP and the Disaster Recovery Plan.	hours beyond the first twenty-four (24) hours. \$6,000 per 24-hour period seventy-three (73) to one hundred sixty-eight (168) hours. \$7,000 per 24-hour period if more than one hundred sixty-eight (168) hours.
B12.26	The Contractor will be held accountable for and must reimburse the Department for any EVV related claims paid as a result of any error on the Contractor's part, which exceed or do not comport with the service limitations or prior authorized amount. Including any penalties that are assessed by a Federal agency due to this error.	Total amount of claims payment that exceeds or does not comport with the service limitations or prior authorized amount plus any penalties that are assessed by a Federal agency.

3.19. Project Duration

- 3.19.1. This Contract is effective upon Governor and Executive Council approval through June 30, 2026.
- 3.19.2. The Department may extend contracted services for up to four (4) additional years contingent upon agreement of the Parties, satisfactory Contractor performance, continued funding, and Governor and Executive Council approval.

3.20. System Requirements

- 3.20.1. The Contractor shall provide the Authenticare EVV System as an open/hybrid model for EVV to track and monitor timely service delivery and access to care for members, while providing flexibility to the State of New Hampshire's providers and managed care organizations. The Authenticare EVV System must include three foundational elements: data collection, data aggregation, and KPI/Metric monitoring.
- 3.20.2. The Authenticare EVV System must be flexible and scalable so that it can easily accommodate the full range of program requirements and user needs, while creating efficiencies by streamlining data and information sharing.
- 3.20.3. The Contractor shall deliver the Authenticare EVV System with data aggregation capabilities that can be utilized by providers and aggregate EVV data from multiple source systems for claims validation and reporting, thereby allowing providers and MCOs with existing EVV systems to continue to use those systems.

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHNICAL REQUIREMENTS AND DELIVERABLES

3.20.4. The Contractor shall assist in determining, providing, monitoring, and reporting Key Performance Indicators.

3.20.5. The Authenticare EVV System must pass CMS certification.

3.21. Data Location

3.21.1. The Selected Contractor shall provide its Services to the State and its end users solely from data centers within the Continental United States. All storage, processing and transmission of State Data shall be restricted to information technology systems within the Continental United States. The Contractor shall not allow its personnel or subcontractors to store State Data on portable devices, including personal computers unless express prior written consent is obtained from the DHHS Information Security Office.

3.22. Background Checks

The Contractor shall conduct criminal background checks, at its own expense, and not utilize any staff, including subcontractors, to fulfill the obligations of the Contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the State's information among the Contractor's employees and agents.

Contractor workforce shall not be permitted to handle, access, view, store or discuss NH DHHS Confidential Data until an attestation is received by the Contractor that all Contractor workforce associated with fulfilling the obligations of this Contract are, based on NH DHHS provided criteria herein and their job responsibility requirements, eligible to participate in work associated with this Contract. The Contractor must provide attestations upon Department request. Contractor agrees it will initiate a criminal background check re-investigation of all workforce assigned to this Contract every five years. The five year period will be based on the date of the last Criminal Background Check conducted by the Contractor or its Agent.

The State may, at its sole expense, conduct reference and background screening of the Contractor's Project Manager and Key Project Staff. The State shall maintain the confidentiality of background screening results in accordance with the Contract.

3.23. Business Requirements

Contractor shall be responsible for meeting the Business Requirements associated with this project as described in Exhibit G, Attachments and Contractor Certificates, Section 1, Attachments, Subsection a., EVV Business and Technical Requirements, Attachment 1.

3.24. Technical Requirements

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHNICAL REQUIREMENTS AND DELIVERABLES

Contractor shall be responsible for meeting the Technical and Security Requirements identified in RFP-2022-DLTSS-05-ELECT and in Exhibit G, Attachments and Contractor Certificates, Section 1, Attachments, Subsection a., EVV Business and Technical Requirements, Attachment I.

4. DELIVERABLE, ACTIVITY, OR MILESTONE

Contractor shall be responsible for meeting the Activities/ Deliverables/Milestones identified in Table B-4:

Table B-4				
ACTIVITY / DELIVERABLES / MILESTONES				
ACTIVITY, DELIVERABLE, OR MILESTONE		DELIVERABLE TYPE	PROJECTED DELIVERY DATE IN DAYS AFTER CONTRACT EFFECTIVE DATE	COMMENTS
PLANNING AND PROJECT MANAGEMENT				
1	Conduct Project Kickoff Meeting	Non-Software	4	
2	Work Plan	Written	7	Initial updates within 2 weeks of Project start
3	Attestation of background check	Written	4	
	Project Status Reports	Written	7	
4	Infrastructure Plan, including Desktop and Network Configuration Requirements	Written	7	
5	Information Security Plan (ISP)	Written	14	
6	Communications and Change Management Plan	Written	14	
7	Bring Your Own Device (BYOD) Security Plan (if applicable and approved by NH DHHS Information Security)	Written	14	
8	Data Protection Impact Assessment (DPIA)	Written	21	

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHNICAL REQUIREMENTS AND DELIVERABLES

9	Software Configuration Plan	Written	21	
10	Systems Interface Plan and Design/Capability	Written	4	
11	Systems Security Plan (SSP)	Written	28	
12	Testing Plan	Written	28	
13	Data Conversion Plan and Design	Written	28	
14	Deployment Plan	Written	35	
15	Disaster Recovery Plan	Written	35	
16	Comprehensive Training Plan and Curriculum	Written	35	
17	End User Support Plan	Written	42	
18	Business Continuity of Operations Plan (COOP)	Written	42	
19	Solutions Requirements Traceability Matrix	Written	21	
20	EVV System Data Retention Plan	Written	42	
21	EVV System Privacy Impact Analysis	Written	49	
22	EVV Solution Reporting User Guide	Written	63	
23	EVV Solution User Manual	Written	63	
24	Operations Support and Management Plan	Written	49	
25	Documentation of Operational Procedures	Written	21	
INSTALLATION				
26	Provide Software Licenses (if needed)	Written	N/A	No licenses needed for SaaS delivery model
27	Provide Fully Tested Data Conversion Software	Software	23	
28	Provide Software Installed, Configured, and Operational to Satisfy State Requirements	Software	74	
TESTING				
29	Conduct Integration Testing	Non-Software	70	
30	Conduct User Acceptance Testing	Non-Software	74	
31	Perform Production Tests	Non-Software	73	

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHNICAL REQUIREMENTS AND DELIVERABLES

32	Test In-Bound and Out-Bound Interfaces	Software	66	
33	Conduct System Performance (Load/Stress) Testing	Non-Software	66	
34	Certification of 3 rd Party Pen Testing and Application Vulnerability Scanning.	Non-Software	53	
35	Security Risk Assessment Report (SRA) if PII is collected on behalf of the State, the SRA shall include a Privacy Impact Assessment (PIA)	Written	53	
36	Security Authorization Package	Written	53	
PILOT DEPLOYMENT				
37	Interfaced Data Loaded into Production Environment	Software	108	
38	Provide Tools for Backup and Recovery of all Applications and Data	Software	N/A	No tools needed by the State - included with AuthentiCare's redundant architecture
39	Operational Readiness Review	Non-Software	92	
40	Conduct Pilot User Training	Non-Software	84	
41	Cutover to New Software	Non-Software	107	
42	First Productive Use – Pilot System Deployment	Non-Software	119	Approximately 4 months after Project Kick-Off
SYSTEM DEPLOYMENT				
43	Converted Data Loaded into Production Environment	Software	196	
44	Provide Tools for Backup and Recovery of all Applications and Data	Software	N/A	No tools needed by the State - included with AuthentiCare's redundant architecture
45	Conduct Training	Non-Software	196	

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHNICAL REQUIREMENTS AND DELIVERABLES

46	Cutover to New Software	Non-Software	207	
47	First Productive Use – Full System Deployment	Non-Software	211	Approximately 3 months after Pilot Go-Live
48	Provide Documentation	Written	196	
49	Execute System Security Plan	Non-Software	73	
50	Lead CMS SMC Certification	Non-Software	505	Approximately 6-9 months after statewide Go-Live
51	Conduct Project Exit Meeting	Non-Software	512	

5. CONTRACT END-OF-LIFE TRANSITION SERVICES

- 5.1. Upon termination or expiration of the Contract the Parties agree to cooperate in good faith to effectuate a smooth secure transition of the Services from the Contractor to the Department and, if applicable, the Contractor engaged by the Department to assume the Services previously performed by the Contractor for this section the new Contractor shall be known as "Recipient"). Contract end of life services shall be provided at no additional cost. Ninety (90) days prior to the end-of the contract or unless otherwise specified by the Department, the Contractor shall begin working with the Department and if applicable, the new Recipient to develop a Data Transition Plan (DTP). The Department shall provide the DTP template to the Contractor that will include termination of interfaces.
- 5.2. The Contractor shall use reasonable efforts to assist the Recipient, in connection with the transition from the performance of Services by the Contractor and its Affiliates to the performance of such Services. This may include assistance with the secure transfer of records (electronic and hard copy), transition of historical data (electronic and hard copy), the transition of any such Service from the hardware, software, network and telecommunications equipment and internet-related information technology infrastructure ("Internal IT Systems") of Contractor to the Internal IT Systems of the Recipient and cooperation with and assistance to any third-party consultants engaged by Recipient in connection with the Transition Services.
- 5.3. If a system, database, hardware, software, and/or software licenses (Tools) was purchased or created to manage, track, and/or store State Data in relationship to this contract said Tools will be inventoried and returned to the Department, along with the inventory document, once transition of State Data is complete.
- 5.4. The internal planning of the Transition Services by the Contractor and its Affiliates shall be provided to the Department and if applicable the Recipient on a timely manner. Any such Transition Services shall be deemed to be Services for purposes of this Contract.

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHNICAL REQUIREMENTS AND DELIVERABLES

5.5. Should the data Transition extend beyond the end of the Contract, the Contractor and its affiliates agree Contract Information Security Requirements, and if applicable, the Department's Business Associates Agreement terms and conditions remain in effect until the Data Transition is accepted as complete by the Department.

5.6. In the event where the contractor has comingled Department Data and the destruction or Transition of said data is not feasible, the Department and Contractor will jointly evaluate regulatory and professional standards for retention requirements prior to destruction.

6. COMPLETION OF TRANSITION SERVICES

6.1. Each service or Transition phase shall be deemed completed (and the Transition process finalized) at the end of 15 business days after the product, resulting from the Service, is delivered to the Department and/or the Recipient in accordance with the mutually agreed upon Transition plan, unless within said 15 business day term the Contractor notifies the Department of an issue requiring additional time to complete said product.

6.2. Once all parties agree the data has been migrated the Contractor will have 30 days to destroy the data per the terms and conditions of the Department's Information Security Requirements Exhibit, including certificate of data destruction.

7. DISAGREEMENT OVER TRANSITION SERVICES RESULTS

In the event the Department is not satisfied with the results of the Transition Service, the Department shall notify the Contractor, by email, stating the reason for the lack of satisfaction within 15 business days of the final product or at any time during the data Transition process. The Parties shall discuss the actions to be taken to resolve the disagreement or issue. If an agreement is not reached, at any time the Department shall be entitled to initiate actions in accordance with this contract.

8. WEBSITE AND SOCIAL MEDIA

Not Applicable

9. STATE OWNED DEVICES, SYSTEMS AND NETWORK USAGE

Not Applicable

10. DELIVERABLE REVIEW AND ACCEPTANCE

10.1. Non-Software and Written Deliverables Review and Acceptance

The Contractor shall provide a written Certification that a non-software, written deliverable (such as the Test Plan) is final, complete, and ready for Review. After receiving such Certification from the Contractor, the State will Review the Deliverable to determine whether it meets the requirements

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHNICAL REQUIREMENTS AND DELIVERABLES

outlined in this Exhibit. The State will notify the Contractor in writing of its Acceptance or rejection of the Deliverable, or its partial or conditional Acceptance of the Deliverable, within five (5) business days of the State's receipt of the Contractor's written Certification; provided that if the State determines that the State needs more than five (5) days, then the State shall be entitled to an extension of up to an additional ten (10) business days. If the State rejects the Deliverable or any portion of the Deliverable, or if any Acceptance by the State is conditioned upon completion of any related matter, then the State shall notify the Contractor of the nature and class of the Deficiency, or the terms of the conditional Acceptance, and the Contractor shall correct the Deficiency or resolve the condition to Acceptance within the period identified in the Work Plan. If no period for the Contractor's correction of the Deliverable or resolution of condition is identified, the Contractor shall correct the Deficiency in the Deliverable or resolve the condition within five (5) business days or such longer period as the State (in its sole discretion) may agree. Upon receipt of the corrected Deliverable, the State shall have five (5) business days to review the Deliverable and notify the Contractor of its Acceptance, Acceptance in part, conditional Acceptance, or rejection thereof, with the option to extend the Review Period up to five (5) additional business days, or mutually agreed upon timeframe. If the Contractor fails to correct the Deficiency within the allotted period, the State may, at its option, continue reviewing the Deliverable and require the Contractor to continue until the Deficiency is corrected, or immediately terminate the Contract, declare the Contractor in default, and or pursue its remedies at law and in equity.

10.2. Software Deliverables Review and Acceptance

System/Software Testing and Acceptance shall be performed as set forth in the Test Plan and more particularly described in Acceptance and Testing Services described herein.

10.3. Number of Deliverables

Unless the State otherwise specifically agrees in writing, in no event shall the Contractor certify for testing and deliver to the State more than three (3) Deliverables for review or testing at one time. As the State accepts a Deliverable, an additional Deliverable may be presented for review but at no time can the Deliverables exceed three (3) at a time without the authorization of the State.

10.4. Conditional and Unconditional Acceptance

By accepting a Deliverable, the State reserves the right to reject any and all Deliverables in the event the State detects any Deficiency in the System, in whole or in part, through completion of all Acceptance Testing, including but not limited to, Software/System Acceptance Testing, and any extensions thereof.

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHINICAL REQUIREMENTS AND DELIVERABLES

11. CHANGE ORDER

- 11.1. The State may make changes, revisions or request enhancements to the Scope of Work at any time by written Change Order. The State originated changes, revisions or enhancements shall be approved by the Department of Information Technology. Within five (5) business days of Contractor's receipt of a Change Order, Contractor shall advise the State, in detail, of any impact on cost (e.g., increase or decrease), the Schedule, and the Work Plan.
- 11.2. Contractor may propose a change within the scope of the Contract by written Change Order, identifying any impact on cost, the Schedule, and the Work Plan. The State shall acknowledge receipt of Contractor's requested Change Order within five (5) business days. The State Agency, as well as the Department of Information Technology, must review and approve all Change Orders in writing. The State shall be deemed to have rejected the Change Order if the Parties are unable to reach an agreement in writing within 30 days of receipt of the Change Order.
- 11.3. Change orders resulting in an increase of Price Limitation, an extension of time for Contract completion or a significant change to the scope of the Contract may require approval by the Governor and Council.
- 11.4. A Change Order which is accepted and executed by both Parties, and if applicable approved by Governor and Council, shall amend the terms of this Agreement.

12. IMPLEMENTATION SERVICES

- 12.1. The Contractor shall employ an industry-standard Implementation strategy with a timeline set forth in accordance with the Work Plan:
- 12.2. The Contractor shall manage Project execution and provide the tools needed to create and manage the Project's Work Plan and tasks, manage and schedule Project staff, track and manage issues, manage changing requirements, maintain communication within the Project Team, and Report status.
- 12.3. The Contractor and the State shall adopt a Change Management approach to identify and plan key strategies, communication initiatives, and training plans.

13. PROJECT MANAGEMENT

The Contractor shall provide project tracking tools and templates to record and manage Issues, Risks, Change Requests, Requirements, and other documents used in the management and tracking of the project. The State believes that effective communication and Reporting are essential to Project success. The Contractor shall employ effective communication and Reporting strategies to ensure Project success. The Contractor Key Project Staff shall participate in meetings as requested by the State, in accordance with the requirements and terms of this Contract.

The Project requires the coordinated efforts of a Project Team consisting of both Contractor and State personnel. Contractor shall provide all necessary resources to perform its obligations under the Contract. Contractor is responsible for providing all appropriate resources and personnel to manage this Project to a successful completion.

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHINICAL REQUIREMENTS AND DELIVERABLES

13.1. The Contractor Key Project Staff

13.1.1. The Contractor's Contract Manager

Contractor shall assign a Contract Manager who will be responsible for all Contract authorization and administration, including but not limited to processing Contract documentation, obtaining executive approvals, tracking costs and payments, and representing the parties in all Contract administrative activities. Contractor's Contract Manager is:

Grant McKay
513-460-8007
Grant.McKAY@Fiserv.com

13.1.2. The Contractor's Project Manager

Contractor shall assign a Project Manager who is qualified to perform or supervise the Contractor's obligations under this Agreement. Contractor's Project Manager is:

John Cutchin
407-893-2557
john.cutchin@Fiserv.com

Contractor's selection of the Project Manager shall be subject to the prior written approval of the State. The State's approval process may include, without limitation, at the State's discretion, review of the proposed Project Manager's resume, qualifications, references, and background checks, and an interview. The State may require removal or reassignment of Project Manager who, in the sole judgment of the State, is found unacceptable or is not performing to the State's satisfaction.

Project Manager must be qualified to perform the obligations required of the position under the Contract, shall have full authority to make binding decisions under the Contract, and shall function as Contractor's representative for all administrative and management matters. Project Manager must be available to promptly respond during normal Business Hours within two (2) hours of inquiries from the State, and be at the site as needed. Project Manager must work diligently and use his/ her best efforts on the Project.

13.1.3. Change of Project Manager

Contractor may not replace the Project Manager or change its assignment of Project Manager without providing the State written notice and obtaining the prior approval of the State of the replacement Project Manager. State approvals for replacement of Project Manager shall not be unreasonably withheld. The replacement Project Manager is subject to the same requirements and Review as set forth above. Contractor shall assign a replacement Project Manager within ten (10) business days of the departure of the prior Project Manager, and Contractor shall continue during the ten (10) business day period to provide competent project management Services through a qualified interim Project Manager.

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHNICAL REQUIREMENTS AND DELIVERABLES

13.1.4. The Contractor's Additional Project Staff

The State considers the following individuals to be Key Project Staff for this Project:

Not Applicable

The State reserves the right to require removal or reassignment of Key Project Staff who are found unacceptable to the State. Contractor shall not change Key Project Staff commitments without providing the State written notice and obtaining the prior written approval of the State. State approvals for replacement of Key Project Staff will not be unreasonably withheld. The replacement Key Project Staff shall have comparable or greater skills than Key Project Staff being replaced.

13.2. The State Key Project Staff

13.2.1. The State Contract Manager

The State shall assign a Contract Manager who shall function as the State's representative with regard to Contract administration. The State Contract Manager is:

Kerri King
603-271-9075
Kerri.L.King@dhhs.nh.gov

13.2.2. The State Project Manager

The State shall assign a Project Manager, or team of Project Managers. The State's Project Manager is:

Cheri Poire
603-271-3792 Cheri.M.Poire@dhhs.nh.gov

And

Kelly Micka
TBD
Kelly.P.Micka@affiliate.dhhs.nh.gov

The State Project Manager's duties shall include the following:

- a. Leading the Project;
- b. Engaging and managing all Contractors working on the Project;
- c. Managing significant issues and risks;
- d. Reviewing and accepting Contract Deliverables;
- e. Invoice sign-offs;
- f. Review and approval of Change Orders;
- g. Managing stakeholders' concerns.

14. WORK PLAN

The Contractor's Project Manager and the State Project manager shall finalize the Work Plan within Fourteen (14) days of the Effective Date and further refine the tasks required to implement the

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHINICAL REQUIREMENTS AND DELIVERABLES

Project. Continued development and management of the Work Plan is a joint effort on the part of the Contractor and State Project Managers.

The preliminary Work Plan created by the Contractor and the State is set forth in this section. The work plan will be finalized with start and end dates as approved by the Department once the project begins.

Table B-5	
Name	Duration
New Hampshire DHHS EVV Project - AuthentiCare Implementation	403 days
Contract Award - Pre-Project	34 days
Milestone: Contractor Selection	0 days
Contract Negotiation and CMS Approval	30 days
Milestone: Contract and BAA Signed	0 days
Milestone: Governor and Council Approval	0 days
Project Initiation	6 days
Assemble Team	1 day
Conduct Project Kick Off Meeting	5 days
Prepare for Project Kick Off Meeting	3 days
Deliverable: Conduct Project Kick Off Meeting	1 day
Document Project Kickoff Outcomes	1 day
Distribute Project Kickoff Outcomes	1 day
Milestone Completed - Project Initiation	0 days
Phase Iteration 1	144 days
Project Planning	0 days
Deliverable: Work Plan	0 days
Create Baseline Project Management Plans, Sub-Plans and Deliverables	0 days
Scope Management Plan	0 days
Cost Management Plan	0 days
Staff Management Plan	0 days
Risk Management Plan	0 days
Issue Management Plan	0 days
Risk Register	0 days

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHINICAL REQUIREMENTS AND DELIVERABLES

Issue Log	0 days
Change Control Log	0 days
Release Management Plan	0 days
Deliverable: Communications and Change Management Plan	0 days
Deliverable: Information Security Plan	0 days
Deliverable: Bring Your Own Device (BYOD) Security Plan	0 days
Deliverable: Data Protection Impact Assessment (DPIA)	0 days
Deliverable: Systems Security Plan	0 days
Deliverable: Infrastructure Plan	0 days
Deliverable: Disaster Recovery	0 days
Deliverable: Business Continuity of Operations Plan	0 days
Deliverable: Status Report Expectation Document - DED	0 days
Collaborate with State - Review and Approve Project Plans and	0 days
Milestone Completed - Project Planning	0 days
Milestone 1: Planning	0 days
Requirements	10 days
Business Requirements Sessions and RTM Creation	10 days
Create Business Requirements Document - BRD	0 days
Requirements Gathering and Clarifications	0 days
Analyze and Validate Business Requirements	0 days
Deliverable: Create Requirements Traceability Matrix - RTM	0 days
Collaborate with State - Review Business Requirements	0 days
Create RTM Baseline - Update with State Feedback	0 days
Business Requirements Document - BRD	0 days
Deliverable: Software Configuration Plan	0 days
Deliverable: Systems Interface Plan and Design/Capability	0 days
Deliverable: EVV System Privacy Impact Analysis	0 days
Deliverable: Data Conversion Plan and Design	0 days
Deliverable: EVV System Data Retention Plan	0 days
Operations Support and Maintenance Plan	0 days
Deliverable: End User Support Plan	0 days
Warranty Plan	0 days
Deliverable: Comprehensive Training Plan and Curriculum	0 days
Deliverable: Test Management Plan	0 days
Collaborate with State - Review and Approve Business Requirements	0 days
Milestone Completed - Requirements	0 days
Design	10 days
Design Sessions	10 days
Review interface specifications and create high level design - HLD	0 days
Collaborate with State - Review and Approve the interface HLD	0 days
Conduct AuthentiCare Design and Configuration Sessions	0 days

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHINCAL REQUIREMENTS AND DELIVERABLES

System Configuration	0 days
Create Detailed Interface Design	0 days
Create IVR Design Flows	0 days
System Customization Design documentation	0 days
Create Development Environment	0 days
Deliverable: Deployment Plan	0 days
Implementation Instructions	0 days
Deployment Checklist	0 days
Back Out (Roll-back) Plan	0 days
Deliverable: Document Operational Procedures	0 days
Deliverable: Operations Support and Management Plan	0 days
Milestone Completed - Design	0 days
Development	20 days
Development	20 days
Create QA Environment	0 days
Perform Custom Configuration and Development	0 days
Perform Data Conversion and Extraction	0 days
Interface Setup and configuration	0 days
Configure and/or Modify Reports	0 days
System Customization Development and Release	0 days
Development Complete	0 days
Release Notes	0 days
Update Test Plan	0 days
Create Regression Testing Scripts and Cases	0 days
Collaborate with State - Review and Approve Updated Test Plan	0 days
Update Test Cases	0 days
Create IVR Call Flows	0 days
Perform IVR Language Translation	0 days
Milestone Completed - Project Development	0 days
Test	40 days
Conduct Quality Assurance Testing	13 days
Deploy to QA environment	3 days
Execute Regression Tests	10 days
Test / Defect Status Report	2 days
Deliverable: Conduct Load/Performance Testing	10 days
Remediate Defects	5 days
QA Complete	0 days
Prepare UAT Environment	29 days
Deliverable: Test Data Import/Conversion	2 days
Create User Acceptance Test (UAT) cases	5 days
Collaborate with State - Review and Approve UAT cases	1 day

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHNICAL REQUIREMENTS AND DELIVERABLES

Deploy Solution to UAT Environment (Web, Mobile, IVR)	2 days
Interface Configuration and Deployment to UAT	2 days
Perform System Validation and Run Smoke Test	1 day
Enable User Onboarding Support for UAT Environment	1 day
Demo system functionality in support of UAT	1 day
Conduct UAT Testing	38 days
Deliverable: Conduct User Acceptance Testing (UAT)	10 days
Support State UAT Outcomes - Remediate Issues	5 days
Conduct Final Resolution of UAT issues Testing	2 days
Review Test Results	1 day
Test Closure Report	2 days
Submit UAT completion for Approval	1 day
Accessibility Sign-off	1 day
UAT Signoff	1 day
Deliverable: Conduct Integration Testing	33 days
Create Integration Test Cases	5 days
Execute Integration Regression Testing	5 days
Deliverable: Test In-bound and Out-bound Interfaces	5 days
Remediate Defects	2 days
Milestone Completed - Test	0 days
Milestone 2: Testing	0 days
Deliverable: Lead CMS Outcomes Based Certification	0 days
CMS SMC Certification Evidence Submission and ORR	38 days
EVV Evidence Gathering	20 days
EVV Evidence Gathering (EVV 1.1 - 7.2, 9.1, 10.1)	20 days
Evidence Gathering (EVV 8.1 Detailed 508 Test Report)	15 days
Deliverable: Penetration Test Report and Security and Privacy Controls	5 days
Penetration Testing	0 days
Deliverable: Security Privacy Risk Assessment Audit (SAR) Report	5 days
Deliverable: Security Authorization Package	0 days
Review Audit Results with State Medicaid Agency	5 days
Submission of Evidence to CMS	3 days
State Schedules ORR Target Date	1 day
Confirmation of ORR Date	1 day
Deliverable: Conduct CMS ORR and Receive Approval	1 day
CMS Approval of ORR	1 day
Milestone Completed - CMS Submission and ORR	0 days
Training	134 days
Training and Outreach	45 days
Contact List Creation (Provider and Contractor)	1 day
Identify Pilot Partners and Contractors	14 days

Page 43 of 72

Contractor Initials: SMDate: 9/2/2022

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHINICAL REQUIREMENTS AND DELIVERABLES

Update Training Plan	3 days
Collaborate with State - Review and Approve Updated Training Plan	3 days
Deliverable: Update AuthentiCare User Manuals	30 days
Deliverable: Update Solution Reporting user Guide	30 days
Create Training Materials	30 days
Translate Training Material to All Required Languages	15 days
Create Training Environment	3 days
Deploy Solution to Training Environment	1 day
Perform System Validation and Run Smoke Test	1 day
Enable User Onboarding Support for Training Environment	1 day
Deliverable: Conduct Training for State Staff	10 days
Deliverable: Conduct Training for Provider and Contractor	20 days
Deliverable: Conduct Training for Pilot users	20 days
Milestone Completed - Training and Outreach	0 days
Contractor Onboarding	98 days
Aggregator Onboarding	60 days
Create Credentials	5 days
Communicate Aggregator Guides and Documents	5 days
Begin Contractor Aggregator Integration Support	60 days
Milestone Completed - Contractor Onboarding	0 days
Production Implementation	28 days
Install Interfaces to Production	1 day
Deliverable: Deploy code to production (New Software)	1 day
Deliverable: Production Validation	1 day
Deliverable: Interface Data Loaded in Production	1 day
Validation of Data Imports and Configuration	1 day
IVR Shakeout	1 day
Mobile Shakeout	1 day
Deliverable: Execute System Security Plan	1 day
Deliverable: Backup and Recovery Configuration Verified	1 day
Deliverable: State Signoff on Deployed Solution	1 day
Milestone Completed - Production Deployment	0 days
Milestone 3: Installation	0 days
Pilot Production Go-Live	26 days
Go-Live Preparation	8 days
Execute Release Management Plan	1 day
Review Defect Report	1 day
Review Risks and Issues	1 day
Review Communications Plan	1 day
Review Support and Maintenance Plan	5 days
Assess Operational Readiness	5 days

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHINCAL REQUIREMENTS AND DELIVERABLES

Review Warranty Plan	1 day
Deliverable: Conduct Operational Readiness Review (ORR)	1 day
Go-Live Preparation Remediation (if required)	1 day
Secure Go / No Go Decision	1 day
Execute Transition Plan	1 day
Pilot	5 days
Configure Pilot User Access	5 days
Deliverable: First Productive Use – Pilot System Deployment	1 day
Milestone Completed - Production Go-live	0 days
Milestone 4: Pilot Go-live	0 days
Post-Production Operations Support	0 days
Warranty Support - 90 Calendar Days Begins	0 days
Ongoing Operational Support Begins	0 days
Ongoing Training for Providers, Recipients and Representatives Begins	0 days
Phase Iteration 2	94 days
Planning (Iteration 2)	10 days
Update Project Work Plan	10 days
Update Risk Register	10 days
Issue Log	10 days
Update Change Control Log	10 days
Update Release Management Plan	10 days
Requirements (Iteration 2)	10 days
Business Requirements Sessions and RTM updates	10 days
Update Business Requirements Document - BRD	10 days
Requirements Gathering and Clarifications	10 days
Analyze and Validate Business Requirements	10 days
Update Requirements Traceability Matrix - RTM	10 days
Collaborate with State - Review Business Requirements	10 days
Update Software Configuration Plan	10 days
Update Operations Support and Maintenance Plan	10 days
Collaborate with State - Review and Approve Business Requirements	10 days
Update Change Requests	10 days
Design (Iteration 2)	10 days
Design Sessions	10 days
Review interface specifications and create high level design - HLD	10 days
Collaborate with State - Review and Approve the interface HLD	10 days
Conduct AuthentiCare Design and Configuration Sessions	10 days
Deliverable: System Configuration	10 days
Create Detailed Interface Design	10 days
Create IVR Design Flows	10 days
System Customization Design documentation	10 days

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHINCAL REQUIREMENTS AND DELIVERABLES

Create Development Environment	10 days
Deliverable: Deployment Plan	10 days
Implementation Instructions	10 days
Deployment Checklist	10 days
Back Out (Roll-back) Plan	10 days
Milestone Completed - Design	0 days
Development (Iteration 2)	10 days
Development	10 days
Update Interface Setup and configuration	10 days
Configure and/or Modify Reports	10 days
Update Regression Testing Scripts and Cases	10 days
Collaborate with State - Review and Approve Updated Test Plan	10 days
Test (Iteration 2)	30 days
Conduct Quality Assurance Testing	10 days
Deploy to QA environment	10 days
Execute Regression Tests	10 days
Test / Defect Status Report	10 days
Remediate Defects	10 days
QA Complete	10 days
Prepare UAT Environment	10 days
Create User Acceptance Test (UAT) cases	10 days
Collaborate with State - Review and Approve UAT cases	10 days
Deploy Solution to UAT Environment (Web, Mobile, IVR)	10 days
Interface Configuration and Deployment to UAT	10 days
Conduct UAT Testing	10 days
Conduct User Acceptance Testing (UAT)	10 days
Support State UAT Outcomes - Remediate Issues	10 days
Conduct Final Resolution of UAT issues Testing	10 days
Review Test Results	10 days
Test Closure Report	10 days
Submit UAT completion for Approval	10 days
UAT Signoff	10 days
Training (Iteration 2)	15 days
Training and Outreach	15 days
Update Training Plan	15 days
Collaborate with State - Review and Approve Updated Training Plan	15 days
Update Create User Manuals	15 days
Create Training Materials	15 days
Conduct Training for State Staff	15 days
Conduct Training for Provider and Contractor	15 days
Production Implementation (Iteration 2)	9 days

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHNICAL REQUIREMENTS AND DELIVERABLES

Deploy code to production	9 days
Production Validation	9 days
State Signoff on Deployed Solution	0 days
Full Go-Live (Statewide)	0 days
Deliverable: First Productive Use - Full Systems Deployment	0 days
Milestone 5: System Deployment and Full Go-Live	0 days
CMS Certification	276 days
Conduct CMS Certification Activities (approx. 9-12 months for CMS)	276 days
Ongoing KPI/Metric Gathering Begins	0 days
Generate and Provide Quarterly Q1 KPIs/Metrics under OBC	10 days
Generate and Provide Quarterly Q2 KPIs/Metrics under OBC	10 days
Generate and Provide Quarterly Q3 KPIs/Metrics under OBC	10 days
Completion of all Required CMS SMC Artifacts	0 days
Final Certification Meeting Preparation	8 days
Evidence Review and Submission	5 days
CMS Final Certification Review	2 days
CMS Final CMS Certification Meeting	1 day
Final Certification Received (TBD, typically 6 -9 months)	0 days
Closeout of Implementation	5 days
Update Closeout and Transition Plans	1 day
Conduct Lessons Learned Review	1 day
Prepare Lessons Learned Report	3 days
Deliverable: Conduct Project Exit Meeting	1 day
Milestone 6: Close Project Implementation	0 days

In conjunction with the Contractor's Project Management methodology, which shall be used to manage the Project's life cycle, the Contractor's team and the State shall finalize the Work Plan at the onset of the Project. This plan shall identify the tasks, Deliverables, major milestones, task dependencies, and a payment Schedule required to implement the Project. It shall also address intra-task dependencies, resource allocations (both State and The Contractor's team members), refine the Project's scope, and establish the Project's Schedule.

15. ACCEPTANCE & TESTING SERVICES

- 15.1 The Contractor shall provide Department staff assigned to User Acceptance Testing (UAT) with the full training curriculum and related documentation, including the AuthentiCare User Manual and detailed user guides. The Contractor will train the Department's UAT team on the EVV solution prior to testing.
- 15.2 The Contractor shall provide the Department with updates to the Requirements Traceability Matrix (RTM) identified during final testing, and must provide the updated Change and Defect Management Plan to confirm clarity for managing system changes and system defects throughout the life of the project.

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHNICAL REQUIREMENTS AND DELIVERABLES

- 15.3 The Contractor shall provide access to FDGS' team of implementation specialists, to work with the Department to develop test scenarios in support of UAT. This will include, but not limited to, providing a pre-UAT EVV demonstration to develop detailed test scenarios to support UAT by Department staff.
- 15.4 With approval from the Department, the Contractor shall participate in the Operational Readiness Review (ORR) and initiate the final production implementation tasks.
- 15.5 The Contractor shall conduct automated regression testing for API testing, using specific tools, as needed, Testing tools may include, but are not limited to:
- 15.6 Tricentis Tosca for automated regression testing.
- 15.7 qTest to trace test cases to requirements and documents defects.
- 15.8 SoapUI for API testing.

16. MAINTENANCE, OPERATIONS AND SUPPORT

16.1. System Maintenance

The Contractor shall maintain and support the System in all material respects as described in the Contract, through the Contract Completion Date. The Contractor shall make available to the State the latest program updates, general maintenance releases, selected functionality releases, patches, and Documentation that are generally offered to its customers, at no additional cost.

16.2. System Support

The Contractor must perform on-site or remote technical support in accordance with the Contract, including without limitation the requirements, terms, and conditions contained herein.

As part of the Software maintenance agreement, ongoing Software maintenance and support levels, including all new Software releases, shall be responded to according to the following:

Class A Deficiencies – The Contractor shall have available to the State on-call telephone assistance, with issue tracking available to the State, eight (8) hours per day and five (5) days a week with an email / telephone response within two (2) hours of request; or the Contractor shall provide support on-site or with remote diagnostic Services, within four (4) business hours of a request;

Class B & C Deficiencies – The State shall notify the Contractor of such Deficiencies during regular Business Hours and the Contractor shall respond back within four (4) hours of notification of planned corrective action.

16.3. Reserved

16.4. Contract Warranties and Representations

16.4.1. System

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHNICAL REQUIREMENTS AND DELIVERABLES

The Contractor warrants that any Systems provided under this Agreement will operate and conform to the Specifications, terms, and requirements of this Agreement.

16.4.2. Software

The Contractor warrants that any Software provided as part of this Agreement, including but not limited to the individual modules or functions furnished under the Contract, is properly functioning within the System, compliant with the requirements of the Contract, and will operate in accordance with the Specifications and terms of the Contract.

For any breach of the above Software warranty, in addition to all its other remedies at law and in equity, at the State's option the Contractor shall:

- a. provide the correction of program errors that cause breach of the warranty, or if Contractor cannot substantially correct such breach in a commercially reasonable manner, the State may end its program license if any and recover the fees paid to Contractor for the program license and any unused, prepaid technical support fees the State has paid for the program license; or
- b. the re-performance of the deficient Services, or
- c. if Contractor cannot substantially correct a breach in a commercially reasonable manner, the State may end the relevant Services and recover the fees paid to Contractor for the deficient Services.

16.4.3. Compatibility

Contractor warrants that all System components, including but not limited to the components provided, any replacement or upgraded System Software components provided by Contractor to correct Deficiencies or as an Enhancement, shall operate with the rest of the System without loss of any functionality.

16.4.4. Services

Contractor warrants that all Services to be provided under this Agreement will be provided expediently, in a professional manner, in accordance with industry standards and that Services will comply with performance standards, Specifications, and terms of the Contract.

17. DATA PROTECTION

17.1 Contractor shall comply with Exhibit G, Attachments and Contractor Exhibits, Section 1, Attachments, Subsection b., DHHS Agency Compliance Documents – Attachment 2, Exhibit K, DHHS Information Security Requirements.

17.2 Privacy Impact Assessment

17.2.1 The Contractor agrees to conduct a Privacy Impact Assessment (PIA) of its system prior to system implementation. The Contractor agrees to use the Department's PIA template and PIA requirements for this deliverable. The PIA shall include, at minimum, the following:

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHNICAL REQUIREMENTS AND DELIVERABLES

- 17.2.1.1 How Personally Identifiable Information (PII) is gathered and stored;
 - 17.2.1.2 Who will have access to PII;
 - 17.2.1.3 How PII will be used in the system;
 - 17.2.1.4 How individual consent will be achieved and revoked; and
 - 17.2.1.5 Privacy practices.
- 17.2.2 The Contractor agrees it shall conduct follow-up PIA's in the event there are either significant process changes or new technologies impacting the collection, processing or storage of PII.

18. SOFTWARE AGREEMENT

The Contractor shall provide the State with access to the Software Licenses and Documentation set forth in the Contract, and particularly described Exhibit D: Software Agreement

19. ADMINISTRATIVE SERVICES

The Contract shall provide the State with the Administrative Services set forth in the Contract, and particularly described in Exhibit E: Administrative Services

20. TRAINING

The Contractor shall provide initial and on-going training to all users, as specified by the Department, in accessible formats and locations. The Contractor must offer and provide user training through a variety of mediums, that includes, but is not limited to:

- a. In-person training at locations Statewide, to be approved by the Department.
- b. An on-line, guided webinar.
- c. Recorded webinar.
- d. A Learning Management system, that must include:
 - i. On-demand training that includes self-paced, web-based training modules available for providers to review different scenarios on demand.
 - ii. A Video Library that includes pre-recorded and customized videos, which demonstrate how to perform various functions for a number of user roles and account for numerous learning styles.
- e. A provider forum for training of enhancements and to allow the provider community an opportunity to brainstorm collaboratively about any suggestions they might have to expand AuthentiCare solution's capabilities.
- f. A User manual that is designed for the Department's EVV programs.

**STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT B – STATEMENT OF WORK
BUSINESS / TECHINCAL REQUIREMENTS AND DELIVERABLES**

- g. A worker guide with instruction for workers to complete the check-in and check-out process on their mobile device, in addition to troubleshooting guidance for common issues.

21. TERMS AND DEFINITIONS

Terms and Definitions applicable to this Contract are identified in Exhibit F: Terms and Definitions.

22. CONTRACTOR'S CERTIFICATES

Required Contractor Certificates are attached in Exhibit G.

Remainder of this page intentionally left blank

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT C – PRICE AND PAYMENT SCHEDULE

EXHIBIT C – PRICE AND PAYMENT SCHEDULE

The terms outlined in the Payment Schedule is set forth below:

1. CONTRACT PRICE

Notwithstanding any provision in the Contract to the contrary, and notwithstanding unexpected circumstances, in no event shall the total of all payments made by the State exceed the amount indicated in P-37 General Provisions - Block 1.8: Price Limitation. The payment by the State of the total Contract price shall be the only, and the complete reimbursement to the Contractor for all fees and expenses, of whatever nature, incurred by the Contractor in the performance hereof.

2. TRAVEL EXPENSES

The State will not be responsible for any travel or out of pocket expenses incurred in the performance of the Services performed under this Contract. The Contractor must assume all travel and related expenses incurred by Contractor in performance of its obligations. All labor rates in this Agreement will be considered "Fully Loaded", including, but not limited to: meals, hotel/housing, airfare, car rentals, car mileage, and any additional out of pocket expenses.

3. SHIPPING FEES

The State will not pay for any shipping or delivery fees unless specifically itemized in this Agreement.

4. INVOICING

The Contractor shall submit correct invoices to the State for all amounts to be paid by the State. All invoices submitted shall be subject to the State's prior written approval, which shall not be unreasonably withheld. The Contractor shall only submit invoices for Services or Deliverables as permitted by the Contract. Invoices must be in a format as determined by the State and contain detailed information, including without limitation: itemization of each Deliverable and identification of the Deliverable for which payment is sought, and the Acceptance date triggering such payment; date of delivery and/or installation; monthly maintenance charges; any other Project costs or retention amounts if applicable.

Upon Acceptance of a Deliverable, and a properly documented and undisputed invoice, the State will pay the correct and undisputed invoice within thirty (30) days of invoice receipt. Invoices will not be backdated and shall be promptly dispatched.

5. INVOICE ADDRESS

Invoices may be sent to:

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT C – PRICE AND PAYMENT SCHEDULE

The Department of Health and Human Services
Financial Manager
Department of Health and Human Services
129 Pleasant Street
Concord, NH 03301

Email: DMSInvoices@dhhs.nh.gov

6. PAYMENT ADDRESS

Payments shall be made via ACH. Use the following link to enroll with the State Treasury for ACH payments: <https://www.nh.gov/treasury/state-Contractors/index.htm>

7. OVERPAYMENTS TO THE CONTRACTOR

The Contractor shall promptly, but no later than fifteen (15) business days, return to the State the full amount of any overpayment or erroneous payment upon discovery or notice from the State.

8. CREDITS

The State may apply credits due to the State arising out of this Contract, against the Contractor's invoices with appropriate information attached.

9. RESERVED

10. PAYMENT SCHEDULE

10.1 Contract Type

10.1.1. Activities / Deliverables / Milestones Pricing

This is a Fixed Firm Price Contract. The total Contract value is indicated in P-37 General Provisions - Block 1.8: Price Limitation for the period between the Effective Date through date indicated in P-37 General Provisions - Block 1.7: Completion Date. The Contractor shall be responsible for performing its obligations in accordance with the Contract. This Contract will allow the Contractor to invoice the State for the following activities, Deliverables, or milestones appearing in the price and payment tables below:

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT C – PRICE AND PAYMENT SCHEDULE

Table 10.1.1

IMPLEMENTATION ACTIVITY / DELIVERABLES / MILESTONES PRICING			
	ACTIVITY, DELIVERABLE, OR MILESTONE	DELIVERABLE TYPE	PRICE
1	Conduct Project Kickoff Meeting	Non-Software	\$3,940.00
2	Work Plan	Written	\$5,910.00
3	Background Check Attestation	Written	\$0
	Project Status Reports	Written	\$3,940.00
4	Infrastructure Plan, including Desktop and Network Configuration Requirements	Written	\$0
5	Information Security Plan (ISP)	Written	\$3,940.00
6	Communications and Change Management Plan	Written	\$3,940.00
7	Bring Your Own Device (BYOD) Security Plan	Written	\$3,940.00
8	Data Protection Impact Assessment (DPIA)	Written	\$0
9	Software Configuration Plan	Written	\$3,940.00
10	Systems Interface Plan and Design/Capability	Written	\$3,940.00
11	Systems Security Plan (SSP) (includes PIA)	Written	\$3,940.00
12	Testing Plan	Written	\$3,940.00
13	Data Conversion Plan and Design	Written	\$3,940.00
14	Deployment Plan	Written	\$3,940.00
15	Disaster Recovery Plan	Written	\$3,940.00
16	Comprehensive Training Plan and Curriculum	Written	\$5,910.00
17	End User Support Plan	Written	\$3,940.00

Page 54 of 72

Contractor Initials: SMDate: 9/2/2022

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT C – PRICE AND PAYMENT SCHEDULE

18	Business Continuity of Operations Plan (COOP)	Written	\$3,940.00
19	Solutions Requirements Traceability Matrix	Written	\$3,940.00
20	EVV System Data Retention Plan	Written	\$3,940.00
21	EVV System Privacy Impact Analysis	Written	\$3,940.00
22	EVV Solution Reporting User Guide	Written	\$3,940.00
23	EVV Solution User Manual	Written	\$3,940.00
24	Operations Support and Management Plan	Written	\$3,940.00
25	Documentation of Operational Procedures	Written	\$3,940.00
26	Provide Software Licenses (if needed)	Written	\$0
27	Provide Fully Tested Data Conversion Software	Software	\$0
28	Provide Software Installed, Configured, and Operational to Satisfy State Requirements	Software	\$0
29	Conduct Integration Testing	Non-Software	\$1,970.00
30	Conduct User Acceptance Testing	Non-Software	\$1,970.00
31	Perform Production Tests	Non-Software	\$0
32	Test In-Bound and Out-Bound Interfaces	Software	\$3,940.00
33	Conduct System Performance (Load/Stress) Testing	Non-Software	\$0
34	Certification of 3rd Party Pen Testing and Application Vulnerability Scanning.	Non-Software	\$0
35	Security Risk Assessment Report, including a Privacy Impact Assessment	Written	\$3,940.00
36	Security Authorization Package	Written	\$0
37	Interfaced Data Loaded into Production Environment	Software	\$3,940.00

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT C – PRICE AND PAYMENT SCHEDULE

38	Provide Tools for Backup and Recovery of all Applications and Data	Software	\$0
39	Operational Readiness Review	Non-Software	\$3,940.00
40	Conduct Pilot User Training	Non-Software	\$3,940.00
41	Cutover to New Software	Non-Software	\$7,880.00
42	First Productive Use – Pilot System Deployment	Non-Software	\$9,850.00
43	Converted Data Loaded into Production Environment	Software	\$1,970.00
44	Provide Tools for Backup and Recovery of all Applications and Data	Software	\$0
45	Conduct Training	Non-Software	\$3,940.00
46	Cutover to New Software	Non-Software	\$7,880.00
47	First Productive Use – Full System Deployment	Non-Software	\$39,400.00
48	Provide Documentation	Written	\$0
49	Execute System Security Plan	Non-Software	\$0
50	Lead CMS SMC Certification	Non-Software	\$3,940.00
51	Conduct Project Exit Meeting	Non-Software	\$3,940.00
TOTAL			\$197,000.00

10.1.2. Hardware Pricing

N/A (included with SaaS delivery model)

10.1.3. Software License Pricing

N/A (included with SaaS delivery model)

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT C – PRICE AND PAYMENT SCHEDULE

10.1.4. Software Operations, Maintenance and Support Pricing

Table 10.1.4

SOFTWARE OPERATIONS, MAINTENANCE, AND SUPPORT PRICING

SOFTWARE NAME	STATE FISCAL YEAR 2023	STATE FISCAL YEAR 2024	STATE FISCAL YEAR 2025	STATE FISCAL YEAR 2026
AuthentiCare EVV and Aggregator Operations, Maintenance and Support	\$306,000.00	\$399,000.00	\$399,000.00	\$399,000.00
Total	\$306,000.00	\$399,000.00	\$399,000.00	\$399,000.00

10.1.5. Hosting Pricing

N/A (included with SaaS delivery model)

10.1.6. Other Cost Pricing

N/A (included with SaaS delivery model)

10.1.7. Implementation Pricing Summary

N/A (Included with Table 10.1.1, above)

10.1.8. Contractor Staff, Resource Hours and Rates Worksheet

N/A (Included with Tables 10.1.1 and 10.1.4, above)

10.1.9. Future Contractor Rates Worksheet

Not Applicable.

10.1.10. Pricing Summary

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT C – PRICE AND PAYMENT SCHEDULE

Table 10.1.10		
PRICING SUMMARY		
COST TABLE #	COST TYPE	TOTAL COST
1	Implementation Activities/Deliverables/Milestones Pricing (Total from Table E 1.1, Implementation Activity/Deliverables/Milestones Pricing Worksheet)	\$197,000.00
2	Hardware Pricing (Total from Table E 1.2, Hardware Pricing Worksheet)	\$0
3	Software License Pricing (Total from Table E.1.3, Software License Pricing Worksheet)	\$0
4	Software Operations, Maintenance, and Support Pricing (Total from Table E 1.4, Software Operations, Maintenance, and Support Pricing Worksheet)	\$1,503,000.00
5	Hosting Pricing (Total from Table E 1.5, Hosting Detail Pricing Worksheet)	\$0
6	Other Pricing (Total from Table E 1.6, Other Cost Pricing Worksheet)	\$0
Grand Total		\$1,700,000.00

Remainder of this page intentionally left blank

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT D – SOFTWARE AGREEMENT

EXHIBIT D – SOFTWARE AGREEMENT

The terms outlined in the Software Agreement are set forth below:

1. LICENSE GRANT

- 1.1 COTS -- Not Applicable (N/A)**
- 1.2 SAAS -- Grant of Rights**

During the Subscription Term, the State will receive a nonexclusive, non-assignable, royalty free, worldwide right to access and use the Software solely for the State's internal business operations subject to the terms of this Agreement and up to the number of Licenses documented in the Agreement.

The Parties acknowledge that this Agreement is a Services agreement and Contractor will not be delivering copies of the Software to Customer as part of the Agreement.

1.3 SUBSCRIPTION -- Not Applicable (N/A)

1.4.1. CUSTOM SOFTWARE -Software Title

The Contractor agrees that any and all work product created pursuant to this Agreement, including but not limited to all Software, are deemed to be "Work For Hire" within the meaning of the Copyright Act of 1976. To the extent Contractor is deemed to have retained any legal title, rights and interest in these works, Contractor hereby assigns any and all such title, rights, and interest (including all ownership and intellectual property rights) in the Software and related work product to the State of New Hampshire in consideration for the promises set forth within this Agreement.

1.4.2. Documentation and Copies

The State shall be entitled to copies of any work product upon request to Contractor. At the conclusion of this Agreement, the Contractor agrees to provide all copies of the Software for all versions, including related Documentation, to the State. Contractor shall not retain any work product associated with this Agreement unless authorized by the State in writing.

1.4.3. Restriction on Use

Unless specifically authorized by the State, Contractor shall not utilize work product derived as part of this Agreement in any manner other than as required by Contractor to complete its obligations under this Agreement.

1.4.4. Software Non-Infringement

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT D – SOFTWARE AGREEMENT

Contractor warrants that the Software, including any all component parts thereof ("Contracted Works") are original works of the Contractor that do not violate or infringe any patent, trademark, copyright, trade name or other intellectual property rights or misappropriate a trade secret of any third party.

1.4.4.1. The warranty of non-infringement shall be an on-going and perpetual obligation that shall survive termination of the Contract. In the event that someone makes a claim against the State that any Contracted Works infringe their intellectual property rights, Contractor shall defend and indemnify the State against the claim provided that the State:

- a. Promptly notifies Contractor in writing, not later than 30 days after the State receives actual written notice of such claim;
- b. Gives Contractor control of the defense and any settlement negotiations; and
- c. Gives Contractor the information, authority, and assistance reasonably needed to defend against or settle the claim.

1.4.4.2. Notwithstanding the foregoing, the State's counsel may participate in any claim to the extent the State seeks to assert any immunities or defenses applicable to the State.

1.4.4.3. If Contractor believes or it is determined that any of the Contracted Works may have violated someone else's intellectual property rights, Contractor may choose to either modify the Contracted Works to be non-infringing or obtain a license to allow for continued use, or if these alternatives are not commercially reasonable, Contractor may end the license, and require return of the applicable Contracted Works and refund all fees the State has paid Contractor under the Contract. Contractor will not indemnify the State if the State alters the Contracted Works without Contractor's consent or uses it outside the scope of use identified in Contractor's user Documentation or if the State uses a version of the Contracted Works which has been superseded, if the infringement claim could have been avoided by using an unaltered current version of the Contracted Works which was provided to the State at no additional cost. Contractor will not indemnify the State to the extent that an infringement claim is based upon any information design, Specification, instruction, Software, data, or material not furnished by Contractor. Contractor will not indemnify the State to the extent that an infringement claim is based upon the combination of any Contracted Works with any products or services not provided by Contractor without Contractor's consent.

1.4.5. Viruses

Contractor shall provide Software that is free of viruses, destructive programming, and mechanisms designed to disrupt the performance of the Software in accordance with the Specifications.

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT D – SOFTWARE AGREEMENT

2. SOFTWARE TITLE

Title, right, and interest (including all ownership and intellectual property rights) in the Software provided under this Agreement, and its associated documentation, shall remain with the Contractor.

3. SOFTWARE AND DOCUMENTATION COPIES

The State shall be entitled to copies of any work product upon request to Contractor. At the conclusion of this Agreement, Contractor agrees to provide all copies of the Software for all versions, including related documentation, to the State. Contractor shall not retain any work product associated with this Agreement unless authorized by the State in writing.

Contractor shall provide the State with a sufficient number of hard copy versions of the Software's associated Documentation and one (1) electronic version in Microsoft Word and PDF format. The State shall have the right to copy the Software and its associated Documentation within its possession for its internal business needs. To the extent that the State does not have possession of the Software, Contractor shall provide a reasonable number of copies of the Software and associated Documentation upon request. The State agrees to include copyright and proprietary notices provided to the State by the Contractor on such copies.

4. RESTRICTIONS

Except as otherwise permitted under the Contract, the State agrees not to:

- a. Remove or modify any program markings or any notice of the Contractor's proprietary rights;
- b. Make the programs or materials available in any manner to any third party for use in the third party's business operations, except as permitted herein; or
- c. Cause or permit reverse engineering, disassembly or recompilation of the programs.

5. VIRUSES

The Contractor shall provide Software that is free of viruses, destructive programming, and mechanisms designed to disrupt the performance of the Software in accordance with the Specifications. As a part of its internal development process, Contractor will use reasonable efforts to test the Software for Viruses.

6. AUDIT

Upon forty-five (45) days written notice, the Contractor may audit the State's use of the programs at the Contractor's sole expense. The State agrees to cooperate with the Contractor's audit and provide reasonable assistance and access to information. The

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT D – SOFTWARE AGREEMENT

State agrees that the Contractor shall not be responsible for any of the State's reasonable costs incurred in cooperating with the audit. Notwithstanding the foregoing, the Contractor's audit rights are subject to applicable State and federal laws and regulations.

7. SOFTWARE NON-INFRINGEMENT

Contractor warrants that it has good title to, or the right to allow the State to use all Services, equipment, and Software, including any all component parts thereof such as third party Software or programs that may be embedded in the Software ("Contracted Resources") provided under this Contract, and that such Services, equipment, and Software do not violate or infringe any patent, trademark, copyright, trade name or other intellectual property rights or misappropriate a trade secret of any third-party.

The Warranty of non-infringement shall be an on-going and perpetual obligation that shall survive termination of the Contract. In the event that someone makes a claim against the State that any Contracted Resources infringe their intellectual property rights, the Contractor shall defend and indemnify the State against the claim provided that the State:

- a. Promptly notifies the Contractor in writing, not later than 30 days after the State receives actual written notice of such claim;
- b. Gives the Contractor control of the defense and any settlement negotiations; and
- c. Gives the Contractor the information, authority, and assistance reasonably needed to defend against or settle the claim.

Notwithstanding the foregoing, the State's counsel may participate in any claim to the extent the State seeks to assert any immunities or defenses applicable to the State.

If the Contractor believes or it is determined that any of the Contracted Resources may have violated someone else's intellectual property rights, the Contractor may choose to either modify the Contracted Resources to be non-infringing or obtain a License to allow for continued use, or if these alternatives are not commercially reasonable, the Contractor may end the License, and require return of the applicable Contracted Resources and refund all fees the State has paid the Contractor under the Contract. The Contractor will not indemnify the State if the State alters the Contracted Resources without the Contractor's consent or uses it outside the scope of use identified in the Contractor's User Documentation or if the State uses a version of the Contracted Resources which has been superseded, if the infringement claim could have been avoided by using an unaltered current version of the Contracted Resources which was provided to the State at no additional cost. The Contractor will not indemnify the State to the extent that an infringement claim is based upon any information design, Specification, instruction, Software, Data, or material not furnished by the Contractor. The Contractor will not indemnify the State to the extent that an infringement claim is based upon the combination of any Contracted Resources with any products or Services not provided by the Contractor without the Contractor's consent.

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT D – SOFTWARE AGREEMENT

8. CONTROL OF ALL COMPONENT ELEMENTS

Contractor acknowledges and agrees that it is responsible for maintaining all Licenses or permissions to use any third-party Software, equipment, or Services that are component parts of any Deliverable provided under this Agreement for the entire Term of the Contract. Nothing within this provision shall be construed to require Contractor to maintain Licenses and permissions for Software acquired by the State directly or through third parties that may be integrated with the Contractor's Deliverables.

9. CUSTOM SOURCE CODE

Should any custom source code be developed, Contractor shall provide the State with a copy of the source code, which shall be subject to the License rights. The State shall receive a worldwide, perpetual, irrevocable, non-exclusive paid –up right and license to use, copy, modify and prepare derivative works of any custom developed software.

10. SOFTWARE ESCROW

Contractor agrees to provide to the State the currently existing source code and any other tools and requirements necessary to create executable or interpretive programs. This information may be provided to the State either directly, with any such protections as required by the Contractor or through a mutually agreed upon Escrow Agreement. Contractor shall be responsible for all costs associated with the Escrow Agreement and the State shall not assume any liability to the Company or Escrow Agent as a result of the Agreement.

Contractor agrees that the State shall be entitled to utilize the source code in its possession and/or demand a release of the source code from the Escrow Agent upon the occurrence of any of the following events ("Release Events"):

- a. The Contractor has made an assignment for the benefit of creditors;
- b. The Contractor institutes or becomes subject to a liquidation or bankruptcy proceeding of any kind;
- c. A receiver or similar officer has been appointed to take charge of all or part of the Contractor's assets;
- d. The Contractor terminates its maintenance, operations, and support services for the State for the Software or has ceased supporting and maintaining the Software for the State whether due to its ceasing to conduct business generally or otherwise, except in cases where the termination or cessation is a result of the non-payment or other fault of the State;
- e. The Contractor defaults under the Contract; or
- f. The Contractor ceases its on-going business operations or that portion of its business operations relating to the licensing and maintenance of the Software.

Upon the occurrence of a Release Event, the Contractor hereby grants the State the right to use, copy, modify, display, distribute, and prepare derivative works of the

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT D – SOFTWARE AGREEMENT

source code, and to authorize others to do the same on behalf of the State (Contractors, agents, etc.), solely for the purpose of completing the performance of the Contractor's obligations under the Contract, including, but not limited to, providing maintenance and support for the Software and subject to the rights granted in this Contract.

Remainder of this page intentionally left blank

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT E – ADMINSTRATIVE SERVICES

EXHIBIT E – ADMINISTRATIVE SERVICES

1. DISPUTE RESOLUTION

Prior to the filing of any formal proceedings with respect to a dispute (other than an action seeking injunctive relief with respect to intellectual property rights or Confidential Information), the Party believing itself aggrieved (the "Invoking Party") shall call for progressive management involvement in the dispute negotiation by written notice to the other Party. Such notice shall be without prejudice to the Invoking Party's right to any other remedy permitted under the Contract.

The Parties shall use reasonable efforts to arrange personal meetings and/or telephone conferences as needed, at mutually convenient times and places, between negotiators for the Parties at the following successive management levels, each of which shall have a period of allotted time as specified below in which to attempt to resolve the dispute:

Table E-1.			
DISPUTE RESOLUTION RESPONSIBILITY AND SCHEDULE TABLE			
LEVEL	CONTRACTOR POINT OF CONTACT	STATE POINT OF CONTACT	CUMULATIVE ALLOTTED TIME
Primary	Project Manager, Director of Project Management	Project Manager, PMO Office	Five (5) Business Days
First	VP Product Management	Director of Division of Long-Term Supports and Services	Ten (10) Business Days
Second	VP Portfolio	Commissioner, Department of Health and Human Services	Fifteen (15) Business Days
Third	VP Portfolio	Commissioner, Department of Information Technology	Fifteen (15) Business Days

The allotted time for the first level negotiations shall begin on the date the Invoking Party's notice is received by the other Party. Subsequent allotted time is days from the date that the original Invoking Party's notice is received by the other Party.

2. ACCESS AND COOPERATION

Subject to the terms of this Agreement and applicable laws, regulations, and policies, the State will provide the Contractor with access to all program files, libraries, personal computer-based Systems, Software packages, Network Systems, security Systems, and hardware as required to complete the contracted Services.

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT E – ADMINSTRATIVE SERVICES

3. RECORD RETENTION

Contractor and its Subcontractors shall maintain all Project records including but not limited to books, records, documents, and other evidence of accounting procedures and practices, which properly and sufficiently reflect all direct and indirect costs invoiced in the performance of their respective obligations under the Contract. Contractor and its Subcontractors shall retain all such records for three (3) years following termination of the Contract, including any extensions. Records relating to any litigation matters regarding the Contract shall be kept for one (1) year following the termination of all litigation, including the termination of all appeals or the expiration of the appeal period.

Upon prior notice and subject to reasonable time frames, all such records shall be subject to inspection, examination, audit and copying by personnel so authorized by the State and federal officials so authorized by law, rule, regulation or Contract, as applicable. Access to these items shall be provided within Merrimack County of the State of New Hampshire, unless otherwise agreed by the State. Delivery of and access to such records shall be at no cost to the State during the three (3) year period following termination of the Contract and one (1) year Term following litigation relating to the Contract, including all appeals or the expiration of the appeal period. Contractor shall include the record retention and Review requirements of this section in any of its subcontracts.

4. ACCOUNTING

Contractor shall maintain an accounting System in accordance with Generally Accepted Accounting Principles (GAAP). The costs applicable to the Contract shall be ascertainable from the accounting System.

5. AUDIT

The Contractor shall allow the State to audit conformance to the contract terms. The State may perform this audit or contract with a third party at its discretion and at the State's expense.

6. MISCELLANEOUS WORK REQUIREMENTS

6.1 State Website Copyright

All right, title and interest in the State WWW site, including copyright to all Data and information, shall remain with the State. The State shall also retain all right, title and interest in any user interfaces and computer instructions embedded within the WWW pages. All WWW pages and any other Data or information shall, where applicable, display the State's copyright.

Remainder of this page intentionally left blank

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT F – TERMS AND DEFINITIONS

EXHIBIT F – TERMS AND DEFINITIONS

The following general contracting terms and definitions apply except as specifically noted elsewhere in this Contract.

TERM	DEFINITION
Acceptance	Notice from the State that a Deliverable has satisfied Acceptance Test or Review.
Agreement	A Contract duly executed and legally binding.
Security Incident	The definition for this term is located in the Information Security Requirements Exhibit.
Confidential Information or Confidential Data	The definition for this term is located in the Information Security Requirements Exhibit.
Contract	An Agreement between the State of New Hampshire and a Contractor, which creates binding obligations for each party to perform as specified in the Contract Documents.

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT F – TERMS AND DEFINITIONS

Contractor Confidential Information	Information the Contractor has clearly identified in writing to the State it claims to be confidential or proprietary.
Data Breach	The definition for this term is located in the Information Security Requirements Exhibit.
Deficiency (-ies)/Defects	A failure, shortcoming or error in a Deliverable resulting in a Deliverable, the Software, or the System, not conforming to its Specifications.
Deliverable	A Deliverable is any Written, Software, or Non-Software Deliverable (letter, report, manual, book, code, or other), provided by the Contractor to the State or under the terms of a Contract requirement.
Documentation	All information that describes the installation, operation, and use of the Software, either in printed or electronic format.
Enhancements	Updates, additions, modifications to, and new releases for the Software or System, and all changes to the Documentation as a result of improvement in quality, value, or extent.
Hosted Services	Applications, IT infrastructure components or functions that organizations access from external service providers, typically through an internet connection.
Hosted System	The combination of hardware, software and networking components used by the Application Service Provider to deliver the Hosted Services.
Identification and Authentication	Supports obtaining information about those parties attempting to log on to a system or application for security purposes and the validation of those users.

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT F – TERMS AND DEFINITIONS

Implementation	The process for making the System fully Operational for processing the Data.
MMIS	The Department's Medicaid Management Information System.
Non-Public Information	Information, other than Personal Information, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the State because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.
Operational	Operational means that the System is ready for use and fully functional, all Data has been loaded; the System is available for use by the State in its daily operations, and the State has issued Acceptance.
Personal Information	The definition for this term is located in the Information Security Requirements Exhibit.
Proposal	The submission from a Contractor in response to the Request for a Proposal.
Security Incident	The definition for this term is located in the Information Security Requirements Exhibit.
Software	All Custom, SAAS and COTS computer programs and applications provided by the Contractor under the Contract.
Software Deliverables	All Custom, SAAS and COTS Software and Enhancements.
Software License	Licenses provided to the State under this Contract.
Software-as-a-Service (SaaS)	The capability provided to the State to use the Contractor's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin-client interface such as a Web browser (e.g., Web-based email) or a program interface. The State does not manage or control the underlying cloud infrastructure including network, servers, Operating Systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT F – TERMS AND DEFINITIONS

Specifications	Written details that set forth the requirements which include, without limitation, the RFP, the Proposal, the Contract, any performance standards, Documentation, applicable State and federal policies, laws and regulations, State technical standards, subsequent State-approved Deliverables, and other specifications and requirements described in the Contract Documents. The Specifications are, by this reference, made a part of the Contract as though completely set forth herein.
State Data	All Data created or in any way originating with the State, and all Data that is the output of computer processing of or other electronic manipulation of any Data that was created by or in any way originated with the State, whether such Data or output is stored on the State's hardware, the Contractor's hardware or exists in any system owned, maintained or otherwise controlled by the State or by the Contractor.
State Fiscal Year (SFY)	The New Hampshire State Fiscal Year (SFY) runs from July 1 of the preceding calendar year through June 30 of the applicable calendar year.
Subcontractor	A person, partnership, or company not in the employment of, or owned by, the Contractor which is performing Services under this Contract under a separate Contract with or on behalf of the Contractor.
System	All Software, specified hardware, interfaces and extensions, integrated and functioning together in accordance with the Specifications.
Term	Period of the Contract from the Effective Date through the Completion Date identified in the P-37 General Provisions or termination.
Verification	Supports the confirmation of authority to enter a computer system application or network.

**STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT F – TERMS AND DEFINITIONS**

Warranty	The conditions under, and period during, which the Contractor will repair, replace, or other compensate for, the defective item without cost to the buyer or user. It also delineates the rights and obligations of both parties in case of a claim or dispute.
Warranty Period	A period of coverage during which the Contractor is responsible for providing a guarantee for products and Services delivered as defined in the Contract.

Remainder of this page intentionally left blank

**STATE OF NEW HAMPSHIRE
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
RFP-2022-DLTSS-05-ELECT -01- 2022-031 - Electronic Visit Verification System
EXHIBIT G – ATTACHMENTS AND CONTRACTOR CERTIFICATES**

EXHIBIT G – ATTACHMENTS AND CONTRACTOR CERTIFICATES

1. ATTACHMENTS

- a. EVV Business and Technical Requirements – Attachment 1.
- b. DHHS Agency Compliance Documents – Attachment 2

2. CONTRACTOR CERTIFICATES

- a. Contractor's Certificate of Good Standing
- b. Contractor's Certificate of Vote/Authority
- c. Contractor's Certificate of Insurance

Remainder of this page intentionally left blank

Exhibit G, Attachment 1
EVV Business and Technical Requirements

BUSINESS REQUIREMENTS					
State Requirements			Vendor		
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
AVAILABILITY AND ASSESSIBILITY					
B1.1	Vendor must comply with Section 504 of the Rehabilitation Act of 1973.	M	Yes	Standard	FDGS operates in accordance with all Federal accessibility and anti-discrimination regulations, including those outlined in the ADA. Annual third-party assessments create VPAT reports among other assessments to provide continued compliance.
B1.2	Vendor must comply with 42 CFR 431.206.	M	Yes	Standard	FDGS complies with all applicable Federal regulations including how the EVV system may affect services for individuals.
B1.3	Vendor must comply with 45 CFR Part 80.	M	Yes	Standard	FDGS operates in accordance with all Federal accessibility and anti-discrimination regulations, including those outlined in the ADA. Annual third-party assessments create VPAT reports among other assessments to provide continued compliance.
B1.4	Vendor must comply with 36 CFR Part 1194.	M	Yes	Standard	FDGS operates in accordance with all Federal accessibility and anti-discrimination regulations, including those outlined in the ADA. Annual third-party assessments create VPAT reports among other assessments to provide continued compliance.
B1.5	Vendor must comply with Americans Disabilities Act of 1990	M	Yes	Standard	FDGS operates in accordance with all Federal accessibility and anti-discrimination regulations, including those outlined in the ADA. Annual third-party assessments create VPAT reports among other assessments to provide continued compliance.
B1.6	Vendor must provide training to New Hampshire DHHS.	M	Yes	Standard	FDGS will provide training to DHHS and Provider Agencies using instructor-led and virtual webinar training sessions, in addition to the AuthenticCare on-demand content library.
B1.7	Vendor must support users in New Hampshire DHHS.	M	Yes	Standard	The AuthenticCare solution includes intuitive, user-friendly screens in both the website and mobile application. Through the AuthenticCare website, authorized users can manage user access, and create, view and modify visits, claims and schedules. Users can download the AuthenticCare mobile application for free on their mobile phones and tablets. The AuthenticCare mobile application is a complete EVV solution, including Store and Forward technology, for collecting visit information in locations that may not have cellular connectivity.
B1.8	The vendor's solution must allow for support of translation services, including help desk support.	M	Yes	Standard	The AuthenticCare help desk accesses a language line when there is a need for translation services in more than 30 languages. FDGS provides AuthenticCare User Manuals and other training documents in English and Spanish.
B1.9	The vendor's solution/service must support for non-English speaking users.	M	Yes	Standard	AuthenticCare Mobile apps and IVR are available in English and Spanish.
B1.10	Vendor must allow users to submit information through multiple devices including web portal, mobile devices and IVR.	M	Yes	Standard	AuthenticCare captures visit data through our mobile apps, IVR phone call and web interface. EVV data captured by third-party vendors is accepted via the internet through our AuthenticCare Aggregator using web services or through manual upload to the AuthenticCare web site. Other data such as providers, members, workers, and authorizations are received through web service, batch file via SFTP on our File Gateway, or manually on our website.
B1.11	Vendor must support transmission of data via limited bandwidth such as cellular.	M	Yes	Standard	Visits captured using the AuthenticCare mobile app use a limited amount of data to be respectful of caregivers' cellular data plans.
B1.12	Vendor must support offline processing whereby if there is a break in communication service the data is stored and can be transmitted when service is restored.	M	Yes	Standard	The Store and Forward feature of our mobile app allows the capture of visits while the caregiver's device is offline. Once connectivity has been restored, visits are automatically submitted to the server. The app displays a banner letting the caregiver know that they are working offline so they know that they will need to connect in order for their visits to be submitted.
B1.13	Vendor must support alternative device/methods used when GPS tracking is not available.	M	Yes	Standard	In rare instances where GPS is not available, AuthenticCare IVR is accessible using a toll free number dedicated to New Hampshire.
B1.14	Vendor must provide training in accessible locations and formats.	M	Yes	Standard	AuthenticCare offers live instructor-led sessions when possible. When not possible, virtual instructor-led training is held via a recorded interactive webinar. Our Learning Management System offers on-demand options through recorded sessions, virtual eLearning modules, and a video library.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

B1.15	Vendor must adhere to the World Wide Web Consortium (W3C) Web Accessibility Initiative.	M	Yes	Standard	AuthentiCare web and mobile completes conformance reviews with a third party for accessibility compliance. Resulting VPAT documents are available upon request by the State.
B1.16	Vendor must provide standard and configurable reporting.	M	Yes	Standard	AuthentiCare includes a widely used reporting suite for department staff, provider agencies, and payers. These reports are available on demand and are configurable to select only the data required, for example, date ranges and particular services, caregivers, providers, or members. Reports can be exported in PDF, EXCEL, CSV, or XML formats. Access to reports is controlled by user roles.
B1.17	RESERVED				Not Applicable
B1.18	Vendor must perform routine monitoring using software tools to measure the efficiency of online storage access and take corrective action as needed to maximize availability, efficiency and other attributes of service.	M	Yes	Standard	Fiserv data centers use monitoring tools in the review of system performance including databases, operating systems, network, and storage. AuthentiCare also incorporates several performance monitors for tracking interface processing time, report generation time, long-running transactions, and component/system load. We use AppDynamics Performance Monitor (APM), a suite of tools to maintain stability and availability of the AuthentiCare solution platform. Appropriate alerts are configured to proactively address potential issues.
B1.19	Vendor must provide performance monitoring and management reporting.	M	Yes	Standard	AuthentiCare's Service Management team produces and delivers a monthly scorecard to the State regarding system performance and other management reporting.
B1.20	The vendor must provide a solution or service that allows the users of the system to submit necessary EVV data in multiple ways.	M	Yes	Standard	AuthentiCare captures EVV data through our mobile apps, IVR, our website. Supporting data such as authorizations and claims is exchanged with partner systems through standard interfaces. EVV data captured by third-party vendors is accepted through our AuthentiCare Aggregator using web services or through manual upload to the AuthentiCare web site.
B1.21	The vendor must provide a solution that allows for submitting data if the primary mode of submission for EVV Data is not working.	M	Yes	Standard	In the event the primary mobile mode of submitting EVV data is not available, AuthentiCare IVR can be used as a backup method by the Direct Care Worker or a Provider Agency may enter visit information manually in the AuthentiCare web site.
B1.22	The vendor must describe the solution to collect and aggregate data from provider EVV or MCO EVV platforms and solutions.	M	Yes	Standard	The AuthentiCare Aggregator accepts visit data from third-party EVV systems. Data can be uploaded through the AuthentiCare website or submitted via API. Success and failure messages and error details are returned to the sender. Our File Layout Designer allows these partners to define their own file formats based on delimiters or field lengths to minimize burden in data submission.
OPERATIONS					
B2.1	Vendor must have previously successfully implemented the EVV solution for a State which is operational and has received or in the process of receiving CMS outcomes based certification.	M	Yes	Standard	Nevada received final, full CMS approval following the Outcomes Based Certification (OBC) approach using AuthentiCare and partnering with FDGS. This was the first full certification under the OBC methodology. We have completed Operational Readiness Reviews for South Carolina and Texas, and are actively helping Arkansas to become CMS certified as well.
B2.2	Vendor must implement a Software as a Service (SaaS) Solution and Vendor must not have a degree of customization that exceeds 15%.	M	Yes	Standard	AuthentiCare is provided under a SaaS model. It is highly configurable to reduce the need for customization. Our previous implementations have included less than 15% customization.
B2.3	Vendor must have the ability to implement the solution in phases, including a pilot.	M	Yes	Standard	FDGS is very experienced in delivering functionality in phases and with pilot periods. For instance, the most recent EVV functionality was successfully implemented in 3 separate phases to deliver minimum impact to the providers and Managed Care Organizations (MCOs). In our experience a phased approach allows states to successfully come into compliance with EVV requirements specified in the 21st Century Cures Act in a short timeframe.
B2.4	Vendor must implement flexible data interfaces (API/Web Services) with the existing State data sources systems of record. These interfaces should remain durable and allow for upgrades or refreshes when new programs are added and/or new systems/technologies are introduced in the underlying source systems.	M	Yes	Standard	As systems vary between states, FDGS will build durable flexible interfaces to interact with the State's documented APIs.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

B2.5	Vendor must include the cost of readiness activities in Appendix E including operational readiness testing, training and outreach, stabilization and organizational change management.	M	Yes	Standard	FDGS has included the cost of the required readiness activities within this proposal. These activities are part of our standard pilot, implementation and post-implementation plans.
B2.6	Vendor must provide total cost of operations and maintenance through June 2026 in Appendix E.	M	Yes	Standard	FDGS has provided the total cost of operations and maintenance for the State Fiscal Years (SFY) through the initial term of the contract through June 2026. All costs of operations and maintenance are included in Appendix E within our FDGS Price Proposal.
B2.7	Vendor must specify operations costs for the following in Appendix E: a) Software Cost for Maintaining and Operating the Software as a Service Environment and meet the federal and State standards set in the RFP b) Cost to support business operations such as help desk, ongoing training, new providers/MCOs, changes in EVV services, and support costs	M	Yes	Standard	FDGS has provided the specified operational costs in Appendix E including all software, hardware, support, training, operations and maintenance.
B2.8	Vendor must provide 1,500 system enhancement pool hours (or propose a reasonable number of hours) for ongoing changes on an annual basis. The cost of these system enhancement pool hours are included in the offeror's price for operations in Appendix E. The Vendor will only be paid for the hours the Department approves to be used from this pool. If upon completion of the SFY and if pool hours remain, at the Department's discretion, all unused pool hours and cost will: a. Be rolled over to the pool for the next year; or b. Be reduced from the Contract along with the unused dollars.	M	Yes	Standard	FDGS includes up to 1,500 system enhancement pool hours annually in Table E-1.4 Software Operations, Maintenance, and Support Pricing. FDGS will work with DHHS at the end of each SFY to agree how to reconcile unused pool hours.
B2.9	Vendor should identify if worker/member devices are included in the proposal and document the breakdown of the total cost of device management in Appendix E including the cost of new devices for workers/members, replacement devices in case of loss, and upgrades due to life and age of the device. Providing worker/member devices is Optional and should be priced separately.	O	Yes	Standard	Our experience is that caregivers using their own mobile devices provides the least burden on providers and caregivers as well as the State. We have found that for Authenticare states who have enacted policies such as landline requirements for IVR, caregivers using mobile is over 70%. These caregivers are using devices owned by themselves or their Provider agency. FDGS has included the price for 100 devices in Table E-1.10 should a small number of workers/members decide not to use the Bring Your Own Device option including the free download of the Authenticare mobile app. If necessary, FDGS can expand the number of devices.
B2.10	Vendor must specify and identify any minimum covered lives for providing a per member per month of operations cost in Appendix E.	M	Yes	Standard	The RFP states 15,000 service recipients across 145 provider agencies. Therefore, the minimum covered lives for a per member per month of operations cost is 15,000 recipients. To allow time to ramp up, the minimum covered lives count will not be imposed until the completion of the Pilot phase; approximately the third month of operations.
B2.11	Vendor must ensure that the SaaS offering is compliant with the latest federal mandated EVV functional and non-functional requirements at no additional cost to the State.	M	Yes	Standard	As Authenticare provides EVV services in multiple states, FDGS is committed to maintaining compliance with federally mandated requirements, included HIPAA/HITECH.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

B2.12	The Contractor must provide an independent third party to perform penetration testing within six (6) months prior to implementation. Contractor agrees to conduct an annual certified penetration testing of databases, website, web-based portals, or systems developed, implemented, managed, or supported as a deliverable for this contract and when additions or changes to functionality impact the security framework, architecture or when a new vulnerability exists. Certification of this testing will be provided to DHHS Information Security. The objective of said Penetration Testing is to identify design and/or functionality issues in infrastructure of systems that could expose Confidential Data, as well as, computer and network equipment and systems to risks from malicious activities. Within 15 days after the annual Penetration Test has been performed, the Contractor will provide DHHS Information Security with a report of security issues that were revealed. Within 45 days of testing the Contractor will provide DHHS Information Security with a remediation plan. DHHS will decide, in consultation with the Contractor, which, if any, security issues revealed from the Penetration Test will be remediated by the Contractor.	M	Yes	Standard	As part of our CMS certification process, FDGS uses an independent third-party to conduct a penetration test annually, last completed in October 2021. Certification of this testing will be made available to DHHS Information Security. FDGS policy requires security scans of our applications at a minimum of every 90 days. Fortify, WebInspect, and Sonatype scans are implemented into our SLDC process and are integrated into our application build process. In addition, our internal independent cyber security team performs automated and manual tests. Policy dictates and change management enforces that applications with Critical or High vulnerabilities cannot be promoted to production. This policy also defines the timelines to address Moderate and Low vulnerabilities. The results of these activities can be communicated with appropriate stakeholders at DHHS.
B2.13	Vendor must preserve and make available all data and records for a period of ten years from the latter of the complete termination of the Contract the partial termination of the Contract or the date of final payment under this Contract unless a longer period of time is required by law.	M	Yes	Standard	At the end of the contract, FDGS will create a backup of the database indicating a retention period of 10 years.
B2.14	Vendor must provide a standard interface to support integration of data with Provider and MCO EVV systems.	M	Yes	Standard	AuthentiCare Aggregator accepts visit data from third-party EVV systems. Data can be uploaded through the AuthentiCare website or submitted via API. Our File Layout Designer allows these partners to define their own file formats based on delimiters or field lengths to minimize burden in data submission.
B2.15	Vendor must comply with the CMS Seven Standards and Conditions and the most current version of CMS's Medicaid Information Technology Architecture (MITA).	M	Yes	Standard	AuthentiCare platform components are designed and deployed with the seven MITA conditions as primary considerations: <ul style="list-style-type: none"> • Modularity Standard • MITA Condition • Industry Standards Condition • Leverage Condition • Business Results Condition • Reporting Condition • Interoperability Condition FDGS has a strong understanding of MITA and emerging industry changes. Our knowledge of MITA and MMIS systems will benefit DHHS in potential projects involving health care information technology and the migration to a modernized platform.
B2.16	The EVV system must have capacity for future expansion to additional populations or services. Additional services and programs may be added to or removed from the EVV implementation throughout the life of this contract. State has the sole authority to determine when and if services and/or programs are added to or removed from the EVV System.	M	Yes	Standard	The AuthentiCare solution has a robust set of configurable options, which in turn lowers costs associated with initial implementation and expansion to additional programs and services in future change orders. Services are configurable through our web interface and can be quickly implemented for use. Populations can be added through file exchanges or submission through web services.
B2.17	Vendor must provide unlimited access via phone or Email to the Vendor technical support staff between the business hours of 8:00am to 5:00pm, Monday thru Friday EST.	M	Yes	Standard	The AuthentiCare Tier 1 Call Center is accessible through email and telephone 8:00 a.m. to 8:00 p.m. Monday through Friday, Eastern Time, excluding holidays, and accesses a language line when there is a need for language translation.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

B2.18	Vendor must provide user support by phone and email during non-business hours.	M	Yes	Standard	AuthentiCare Tier 2 Help Desk Specialists are on call 24/7 to resolve or escalate issues that occur outside of standard business hours. Calls and emails to the AuthentiCare Help Desk outside of standard business hours will be routed to a Tier 2 Help Desk Specialist to support evenings, weekends and holidays for technical application concerns.
B2.19	The Vendor will provide a completed Security Audit Report with results to the Department each year. The Security Audit Report must include either an electronic data processing (EDP) systems audit using SSAE - 18 at a minimum level service organization control (SOC) 2 Type II or a NIST 800-53 rev 4 assessment at a "moderate" system risk control level.	M	Yes	Standard	FDGS has developed and maintains an industry leading standard EVV System Security Plan (SSP) that serves our existing clients. FDGS will develop the Security Audit Report based on our SSP and active monitoring of New Hampshire AuthentiCare system components and provide to DHHS annually. We will examine NIST 800-53 rev 4 for additional guidance for the Security Audit Report. The AuthentiCare platform is independently audited each year to produce an SSAE 18/SOC 2 Type 2 report. The report covers confidentiality, integrity and availability controls. Due to the sensitive nature of AuthentiCare's annual SSAE 18/SOC 2 Type 2 report, FDGS agrees to provide a shareable version upon request from DHHS. We maintain a documented security plan that is regularly audited by the FFIEC, our Payment Card Industry (PCI) assessor, and under SSAE 18 by Deloitte and Touche. Fiserv/FDGS security plans and procedures are prepared at a facility level, where the AuthentiCare solution is hosted in large scale, redundant data centers.
B2.20	RESERVED				Not Applicable
B2.21	RESERVED				Not Applicable
B2.22	Vendor must ensure seamless coordination and integration with components, other State systems and allow interoperability with provider EVV systems.	M	Yes	Standard	Existing AuthentiCare interfaces and its Aggregator module will provide the required integration.
B2.23	Vendor must provide a written report and assessment to the Department within 24 hours following the identification of any Security Incident detailing all actions taken concerning the incident, including the type of incident, the current status, and any potential impact(s).	M	Yes	Standard	Our Cyber Security Incident Response Plan includes steps for timely identification, investigation, reporting and resolution of incidents, as well as communication to the affected parties. FDGS will provide a written report and assessment to the Department within 24 hours of the confirmation of any Security Incident, detailing all actions taken, the type of incident, current status and any potential impacts.
B2.24	Vendor must ensure that the Agency-defined data extract is supplied accurately to the Data Warehouse/Enterprise Business Intelligence platform. The Vendor shall supply the response file(s) in the format requested by the Agency by the date and time (weekly) agreed upon.	M	Yes	Standard	FDGS will configure our current data extract process to meet requirements for the Agency's Data Warehouse / Enterprise Business Intelligence (EBI) platform. We will work with DHHS on an agreed upon schedule.
B2.25	Vendor must perform patching and corrections to mitigate security vulnerabilities of a critical nature within three Business Days and those of a major nature within 10 Business Days. The Department will determine the level of criticality in consultation with the system vendor.	M	Yes	Standard	FDGS and our Vulnerability Management Services team under our Cyber Security unit will consult with the Department on the determination of the criticality of vulnerabilities. Based on our agreed level of severity, patching and corrections will be implemented on an agreed upon timeline.
B2.26	RESERVED				Not Applicable
B2.27	Vendor must provide an ANSI/TIA-942 Tier 3 Data Center or equivalent.	M	Yes	Standard	Our Chandler and Omaha Data Centers are built to ANSI/TIA-942 standards.
B2.28	The Vendor shall conduct a Go-Live Readiness Review two (2) weeks prior to go-live and for major system releases.	M	Yes	Standard	FDGS communicates release details for major updates to AuthentiCare to all our clients. We will work with the Department to schedule and prepare for Go-Live Readiness Reviews at least two (2) weeks prior to the scheduled release.
B2.29	The Department and the Vendor must both agree that the Vendor's solution meets the system acceptance criteria for First Productive Use - Full System Deployment.	M	Yes	Standard	FDGS will work with DHHS to define the system acceptance criteria prior to Full System Deployment. The approved system acceptance criteria is validated as part of the UAT exit criteria.
DATA AGGREGATOR					

Exhibit G, Attachment 1
EVV Business and Technical Requirements

B3.1	The Vendor must provide for a data aggregation functionality to collect and process data in a secure and real time basis from certified alternative EVV Systems used by Providers or MCOs and approved by the State.	M	Yes	Standard	AuthentiCare Aggregator accepts visits and claims from third-party systems. Data can be uploaded through the AuthentiCare website or submitted via API. Our File Layout Designer allows these partners to define their own file formats based on delimiters or field lengths. FDGS will work with DHHS to document certification and approval requirements for third-party EVV systems.
B3.2	The Vendor aggregator functionality must validate the data submitted by third party EVV systems against business rules. The business rules and the minimum required data set may vary by service/program.	M	Yes	Standard	AuthentiCare Aggregator uses business rules to validate submitted visit data and return results to the supplier for correction of rejected data.
B3.3	The Vendor must generate metrics, management and control reports to provide feedback to third party EVV systems and providers.	M	Yes	Standard	Results are delivered back to the third-party systems through a similar mechanism to the submission. For example, if a vendor submits aggregated data via API, results reports are returned via API. If a vendor submits through manual upload to the AuthentiCare website, results reports are retrieved through the web site. FDGS provides a Monthly Scorecard to DHHS which includes metrics on aggregated data. We will work with DHHS to determine additional metrics required to give feedback to third-party vendors and providers.
B3.4	The Vendor must allow for distinctions between the requirements for alternate data collection systems utilized by Medicaid providers and those utilized by Medicaid Managed Care Organizations.	M	Yes	Standard	Standard interfaces are available for each external system to use for data submission. Third-party systems submitting data on behalf of MCOs typically utilize our standard Encounter interface, while systems submitting data for Medicaid providers generally use our Claim interface. The AuthentiCare Aggregator has separate, configurable workflows for Encounter and Claim submissions that allow states to apply the appropriate set of business rules depending on the type of submission. Our File Layout Designer can be used by these organizations to define their own file formats selecting delimiters or fixed length within the Claim or Encounter submission.
B3.5	The Vendor will have the capability to generate, process and accept 837 EDI transactions to support data aggregator functions.	M	Yes	Standard	AuthentiCare generates 837 EDI transactions typically accepted and processed by payment systems such as MMIS or MCOs. FDGS will develop as per the State's companion guide a process to import 837 EDI transactions from third-party vendors. Within the 837, AuthentiCare will receive the date of service, provider agency, rendering provider, member and service. Complete EVV data, such as check in and check out time and verified location coordinates, will need to be submitted separately through the AuthentiCare Aggregator to meet CMS requirements, if not included on the 837.
B3.6	The vendor must develop specifications to on-board third party EVV systems proposed by Medicaid providers and Medicaid MCOs that are approved by the State. The Vendor must test and implement data interfaces from/to Medicaid providers and MCOs.	M	Yes	Standard	FDGS has standard onboarding, training, and documentation to facilitate the submission of EVV data collected by 3rd party systems through our AuthentiCare Aggregator which collected 900k visits in 2021.
B3.7	Vendor must support monitoring including comparing visit to claims data.	M	Yes	Standard	In AuthentiCare visits and claims are tightly coupled to provide confidence that the appropriate billing has been submitted. This process includes Provider Agency billing confirmation prior to inclusion in the 837 claim file. Reporting and dashboards are available to Providers and DHHS to facilitate validation activities. For example, Providers often use the Billing Invoice report to monitor visits submitted for billing by service date, along with billing status and amount. Providers utilize our Remittance Advice and Remittance Data Listing reports to validate that each visit was adjudicated as expected.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

B3.8	The Vendor must provide technical and operations support for data integration implementation and operations with third party EVV systems used by MCOs and Providers	M	Yes	Standard	FDGS provides this type of support in Arkansas and Nevada to third-party EVV vendors and associated providers using AuthentiCare Aggregator. We first provide vendors with our Aggregator Toolkit, which includes specifications for data submission methods, data elements and file layout. Our technical staff meets with the prospective vendor to guide them through selection of a data transfer method, obtaining testing credentials, submission of first test files and validation of proper transfers. Once all required onboarding steps are complete and all testing issues remediated, our technical support staff confirm readiness and authorize access to begin submitting data to the Production environment.
B3.9	The vendor shall support implementation, testing and re-testing of interfaces with the external systems (e.g., State system of record(s), third party EVV systems) as those systems are modified, upgraded or replaced.	M	Yes	Standard	FDGS understands that external systems may change over the life of our contract and will provide the required support for future modifications through our change order process with additional effort applied toward the 1,500 annual modification hours. The level of effort for these changes depends on the exact nature of the modification to the external system.
B3.10	The Vendor must support testing and on-boarding of new EVV systems proposed by Medicaid Providers and MCOs.	M	Yes	Standard	FDGS will follow agreed-upon standard onboarding process for third-party EVV systems to support new EVV systems proposed by Medicaid Providers and MCOs.
B3.11	RESERVED				Not Applicable
B3.12	If the Vendor determines that the provider's EVV system is not in compliance with the 21st Century CURES Act then the Vendor will bring it to the attention of the State.	M	Yes	Standard	FDGS agrees that if we determine that the provider's EVV system is not in compliance with the 21st Century CURES Act, we will bring it to the attention of the State.
DATA QUALITY					
B4.1	Vendor must provide conceptual and logical data models for all EVV data entities including meta data and data dictionary.	M	Yes	Standard	FDGS will provide information on EVV data available while protecting our intellectual property that could pose a security risk to our other customers.
B4.2	Vendor must support the data requirements of quality improvement organizations established under Part B of Title XI of the Patient Protection and Affordable Care Act.	M	Yes	Standard	FDGS' AuthentiCare CMS Outcomes Based Certification process collects the 6 required data elements and can transmit them to the MIMIS in an agreed upon format.
B4.3	Vendor must provide data governance structure, resources and process, with state participation, to promote data quality and reliability of EVV data.	M	Yes	Standard	In support of all AuthentiCare customers, data quality is of utmost importance. FDGS will work with the State to validate and promote data quality and reliability.
B4.4	Vendor must manage data quality metrics as approved by the state for EVV data: • accessibility • accuracy • completeness • clarity • reliability • relevance • timeliness • uniqueness • validity • value	M	Yes	Standard	The monthly operations scorecard will be reviewed and approved by the State as meeting the quality process and checks for at least the data quality metrics included in this requirement. We will verify that each metric is defined clearly for reporting on the monthly scorecard.
B4.5	Vendor must provide conceptual and logical data models for entities including: • accounts • authorizations • cases • disclosures • transaction logs (user and system) • payments • services • service/care plans • visits	M	Yes	Standard	FDGS will provide information on EVV data structures available while protecting our intellectual property that could pose a security risk to our other customers.
B4.6	Vendor must provide metadata definitions for data entities.	M	Yes	Standard	FDGS will provide information on EVV data definitions available while protecting our intellectual property that could pose a security risk to our other customers.

RFP-2022-DLTSS-05-ELECT -01 #2022-031

First Data Government Solutions, Limited Partnership

Exhibit G, Attachment 1, EVV Business and Technical Requirements

Contractor Initials: SM Page 7
Date: 9/2/2022

Exhibit G, Attachment 1
EVV Business and Technical Requirements

B4.7	Vendor must provide configuration management capabilities.	M	Yes	Standard	AuthentiCare is a highly configurable solution allowing DHHS to determine their own business rules and minimize the need for code modifications.
B4.8	Vendor must manage data quality functions (data validation, data cleansing) for all data within the EVV System.	M	Yes	Standard	Data quality is managed within AuthentiCare using validation and business rules.
B4.9	Vendor must implement system and process controls for all inbound and outbound data interfaces to ensure accurate and secure data exchange between the State and third party systems. The vendor must implement metrics to ensure the accuracy of these interfaces. The State system(s) of record will prescribe the interface specifications to the EVV vendor.	M	Yes	Standard	AuthentiCare includes secure inbound and outbound data exchanges today. FDGS will share the interface specifications to take advantage of existing interfaces as much as possible. FDGS will work with the State to understand and implement to the prescribed interface specifications and associated metrics. Once FDGS receives the interface specifications, we can determine the level of effort and timeline needed to implement the system and process controls and metrics to ensure the accuracy of these interfaces.
B4.10	Vendor must allow users to submit visit verification information.	M	Yes	Standard	Visit verification information is accepted by AuthentiCare through our mobile apps, IVR, website and Aggregator.
B4.11	Vendor must send verified and accurate EVV data to state directed reporting and analytical systems.	M	Yes	Standard	AuthentiCare will be the single system of record for DHHS EVV. As we do for our other clients, verified and accurate data will be interfaced with state directed reporting and analytical systems using standard APIs where available. FDGS will develop additional interfaces during the implementation phase of your project based on requirements gathered during that time.
B4.12	Vendor must have the capability to exchange and interface data with systems of record (e.g., prior/service authorization systems, member, provider and claim processing systems) and have the flexibility to receive the information in multiple formats and frequency. The vendor must support a push or a pull model for data exchange as required by the system of record.	M	Yes	Standard	With preference to established interface capabilities, FDGS will provide the required support for these yet to be defined interfaces. AuthentiCare supports both push and pull of data from external systems via web service and batch file exchanges through our secure file gateway. During implementation we will document the scheduling of these activities. Depending on the data to be exchanged, we will define if a scheduled batch, on demand, or real-time is most appropriate.
B4.13	RESERVED				Not Applicable
B4.14	Vendor must support data collection and verification when services cross calendar days.	M	Yes	Standard	AuthentiCare supports visits that cross calendar days and is configurable to maintain them as a multiday visit or can split them into two days with the first ending at midnight and the second beginning at midnight.
B4.15	Vendor must support ability to collect visit data elements when the Direct Care Worker (DCW) initiates the visit including when there is a visit for a service for which there is no authorization.	M	Yes	Standard	Understanding that the authorizations do not always arrive in a timely manner, AuthentiCare does not prevent a visit from being captured. In a typical implementation, unauthorized visits are not submitted to the payment system as they will likely be denied. The visits are held in AuthentiCare until the authorization has been received at which time it is automatically connected to the visit and allowed to be submitted for payment.
B4.16	Vendor must support data collection and verification for variable locations to include: 1) services in a location other than the members residence. This may be a routine location for service delivery (e.g. the place of employment) or occasional location for service delivery (e.g. a visit to a family members home grocery store); 2) Location verification needs to only occur at the beginning and ending of each shift and does not include ongoing monitoring of a members location throughout the shift.	M	Yes	Standard	AuthentiCare EVV collects visit data regardless of location and supports multiple locations of record for members. The system is designed to allow service to be delivered. Visits can take place in the home or community. They can begin in one location and end in another. Workflow business rules after the visit are configurable to prevent submission of visit based on DHHS and Payer requirements. The location is only monitored/recorded at check in and check out or if the mobile app member lookup feature is used for ease of finding nearby members for check in.
B4.17	The provider in the EVV visit record must be approved for the member and match the one in the claim / encounter submission.	M	Yes	Standard	Provider-member relationships are established based on data received from the State or MCO. Typically this takes place through the authorization. AuthentiCare also supports the ability of the Provider to establish the relationship through our web site or data exchange.
B4.18	Vendor must ensure verification of data for visits to a member on a given day by multiple direct care workers and/or providers.	M	Yes	Standard	AuthentiCare supports visits from multiple workers and/or providers on the same day.

RFP-2022-DLTSS-05-ELECT-01 #2022-031

First Data Government Solutions, Limited Partnership

Exhibit G, Attachment 1, EVV Business and Technical Requirements

Contractor Initials: SM Page 8
Date: 9/2/2022

Exhibit G, Attachment 1
EVV Business and Technical Requirements

B4.19	Vendor must ensure verification of data for the same service provided to a member by more than one direct care workers and/or providers at the same time (i.e. 2:1 staffing ratios consistent with State guidelines policies and manuals including any additions or updates thereto).	M	Yes	Standard	AuthentiCare supports visits from multiple workers and/or providers at the same time.
B4.20	Vendor must ensure verification of data for multiple services provided to the member by multiple direct care workers and/or providers during the same shift.	M	Yes	Standard	AuthentiCare supports visits for multiple services provided by multiple workers and/or providers in the same shift.
B4.21	Vendor must ensure verification of data for multiple services provided to the member by the same direct care worker during the same shift.	M	Yes	Standard	AuthentiCare supports visits with multiple services from the same worker during the same shift.
B4.22	Vendor must ensure verification of data for multiple visits by a single direct care worker and/or provider to a single member per day.	M	Yes	Standard	AuthentiCare supports multiple visits by a single worker and/or provider to a member in a day.
B4.23	Vendor must ensure verification of data for visits to a member that account for living arrangements where multiple members reside at a single address.	M	Yes	Standard	AuthentiCare supports visits for multiple members living at the same location. Each member has a unique identifier and their own addresses facilitating capture of visits for each individual.
B4.24	Vendor must ensure verification of data for visits to multiple members on a given day by a single direct care worker and/or provider.	M	Yes	Standard	AuthentiCare supports visits for workers delivering service to multiple members in a day.
B4.25	Vendor must ensure verification of data for services provided to a group of members at the same location during a single visit consistent with the State guidelines policies and manuals including any additions or updates thereto on group visits.	M	Yes	Standard	AuthentiCare supports visits for workers providing services to multiple members at the same location. Workflow business rules will be configured to meet State guidelines to prevent claim submission for those that are out of compliance.
B4.26	Vendor must ensure verification of data for services provided to a member in situations in which the member and direct care worker reside at the same address.	M	Yes	Standard	AuthentiCare supports visits for workers when they reside at the same address as the member.
B4.27	RESERVED				Not Applicable
COMPLIANCE					
B5.1	Vendor must comply with Section 12006(a) of the 21st Century Cures Act that mandates that states implement EVV for all Medicaid personal care services (PCS) and home health services (HHCS) that require an in-home visit by a provider. This applies to PCS provided under sections 1905(a)(24), 1915(c), 1915(i), 1915(j), 1915(k), and Section 1115; and HHCS provided under 1905(a)(7) of the Social Security Act or a waiver.	M	Yes	Standard	AuthentiCare EVV is in compliance with 21st Century Cures Act mandates and achieved CMS certification under the Outcomes Based Certification process with the State of Nevada.
B5.2	Vendor and all downstream sub vendors or entities must comply with the HIPAA privacy security and breach notification regulations and applicable state and federal laws and regulations for creating, collecting, disclosing, accessing, maintaining, storing and using electronic PHI/PII.	M	Yes	Standard	FDGS complies with applicable regulations and state and federal laws, HIPAA/HITECH independent third-party audits are conducted on the AuthentiCare environment annually.
B5.3	Vendor is required to report any referral of potential fraud or abuse by a provider or their employee to DHHS within 3 business days of the notification.	M	Yes	Standard	FDGS will notify the State in writing within 3 business days following detection by our staff or any referral of fraud or abuse and provide supporting documentation.
B5.4	Vendor must adhere to data retention requirements cited in 45 CFR 164.316 and Administrative Rule 37.85.414. The Department may require a longer retention period on an exception basis to support ongoing business needs.	M	Yes	Standard	All FDGS data is subject to a documented retention plan. FDGS adheres to the HIPAA regulatory requirement of 6 years data retention or longer, as required by the Department.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

B5.5	Vendor must comply with all sections of the Americans with Disabilities Act (ADA), Section 508 of the Rehabilitation Act and ensure user interface standards account for the various forms of colorblindness.	M	Yes	Standard	AuthentiCare is reviewed by an independent third party for ADA 508/WCAG 2.0 Level AA conformance and can provide the VPAT produced by our vendor for the web site and both iOS and Android mobile apps. Our vendor has advised that, while specific disabilities are not referenced within WCAG, Success Criteria 1.4.1 Use of Color, 1.3.3 Sensory Characteristics and 1.4.3 Contrast (Minimum) are sufficient to address the needs of people who are colorblind.
B5.6	Vendor must be knowledgeable of and support the Department to maintain compliance with the "to be" vision of MITA 3.0 Standards and Conditions-MITA Condition or the latest MITA version that requires states to align to and advance in MITA maturity for business, architecture and data.	M	Yes	Standard	AuthentiCare architecture follows MITA 3.0 guidelines and advances the Department's MITA maturity for business, architecture and data. HIPAA/HITECH independent third party audits are conducted on the AuthentiCare environment annually.
B5.7	Vendor must be knowledgeable of and support the Department to maintain compliance with the "to be" vision of MITA 3.0 Standards and Conditions- Industry Standards Condition or the latest MITA version that requires states to align to and advance in MITA maturity for business, architecture and data. Vendor must ensure alignment with, and incorporation of, industry standards, HIPAA, privacy and transaction standards; accessibility standards, and standards that provide greater accessibility for individuals with disabilities and standards under the Affordable Care Act.	M	Yes	Standard	AuthentiCare architecture follows MITA 3.0 guidelines and advances the Department's MITA maturity for business, architecture and data. HIPAA/HITECH independent third party audits are conducted on the AuthentiCare environment annually. AuthentiCare is reviewed by an independent third party for ADA 508/WCAG 2.0 Level AA conformance and can provide the VPAT produced by our vendor for the web site and both iOS and Android mobile apps.
B5.8	Vendor must be knowledgeable of and support the Department to maintain compliance with the "to be" vision of MITA 3.0 Standards and Conditions- Leverage Condition or the latest MITA version that requires states to align to and advance in MITA maturity for business, architecture and data. Vendor must promote sharing, leveraging, and reuse of healthcare technologies and systems within and among states.	M	Yes	Standard	AuthentiCare architecture follows MITA 3.0 guidelines and advances the Department's MITA maturity for business, architecture and data. HIPAA/HITECH independent third party audits are conducted on the AuthentiCare environment annually. AuthentiCare exchanges data with state MMIS, MCOs and other systems including data warehouses, and supports standard interface formats, such as X12 EDI. The product is regularly enhanced to benefit all state customers.
B5.9	Vendor must be knowledgeable of and support the Department to maintain compliance with the "to be" vision of MITA 3.0 Standards and Conditions- Interoperability Condition or the latest MITA version that requires states to align to and advance in MITA maturity for business, architecture and data. The system vendor's solution shall ensure seamless coordination and integration with components, other State systems and allow interoperability with provider EVV systems.	M	Yes	Standard	AuthentiCare architecture follows MITA 3.0 guidelines and advances the Department's MITA maturity for business, architecture and data. HIPAA/HITECH independent third party audits are conducted on the AuthentiCare environment annually. AuthentiCare exchanges data with state MMIS, MCOs and other systems including data warehouses, and supports standard interface formats, such as X12 EDI.
B5.10	Vendor must be knowledgeable of and support the Department to maintain compliance with the "to be" vision of MITA 3.0 Standards and Conditions- Modularity Standard or the latest MITA version that requires states to align to and advance in MITA maturity for business, architecture and data. The system vendor's solution shall use a modular, flexible approach to systems development, including the use of open interfaces and exposed Application Programming Interfaces (API); the separation of standardized business rule definitions from core programming; and the availability of standardized business rule definitions in both human and machine-readable formats.	M	Yes	Standard	AuthentiCare EVV is aligned with MITA principles and architected with a modular design managing data access via role definition and authority. AuthentiCare is audited by independent third parties meeting requirements for MARS-E, CMS OBC and SOC 2 annual certifications. AuthentiCare uses a modular, flexible approach to systems development. This includes the use of open interfaces and exposed application programming interfaces (APIs) to separate business rules from core programming. It also makes business rules available in both human and machine-readable formats. Most business rules in AuthentiCare are captured in metadata tables in the database so they are easily edited and updated as business rules change.
B5.11	The system vendor must provide the Department with compliance assurances for the system vendors scope of work.	M	Yes	Standard	FDGS's independent third party auditors provide detailed reports of our compliance requirements including but not limited to SOC 2, PCI-DSS, HIPAA/HITECH and CMS OBC.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

B5.12	Vendor must be compatible with multiple standard browsers in accordance to the State's IT Standards. The solution shall allow access from standard browsers without requiring specialized plug-ins or applets to function. The solution shall allow for a mobile app that is available through standard Apple and Google App Store.	M	Yes	Standard	AuthentiCare web is supported on industry standard browser and their previous 2 versions including Microsoft Edge, Apple Safari, Google Chrome and Mozilla Firefox without need for specialized plugins or applets. AuthentiCare mobile is available for download at no charge from both the Google Play and Apple app stores.
B5.13	Vendor must maintain an auditing system and employ accounting/auditing procedures and practices that conform to GAAP and GAAS. All charges applicable to the contract shall be readily ascertainable from such records.	M	Yes	Standard	FDGS agrees to maintain an auditing system and employ accounting/auditing procedures and practices that conform to GAAP and GAAS. FDGS follows GAAP accounting procedures today and our auditors follow GAAS when auditing Fiserv/FDGS.
B5.14	Vendor must ensure that all technologies implemented are in compliance with End User Licensing Agreements or other licensing arrangements vendor has entered into.	M	Yes	Standard	FDGS policy requires compliance with our vendor's license agreements.
B5.15	Vendor must comply with Affordable Care Act Section 1104 Administrative Simplification, and Section 1561 Health IT Enrollment Standards and Protocols.	M	Yes	Standard	Along with the requirements of the 21st Century Cures Act, AuthentiCare complies with ACA Sections 1561 and 1104 regarding HIPAA security and privacy standards. The AuthentiCare platform provides world-class security with a proven track record for proactive security and privacy protection.
B5.16	Vendor must develop and maintain procedures for making referrals for suspected fraud, waste, or abuse directly to the Department. The procedures must be submitted to the Department for approval prior to implementation. The procedures must include: a. Educating Vendor staff at all levels, on ways to recognize possible fraud, waste, and abuse; b. Providing the ability for Vendor staff, at all levels, to freely and directly refer all instances of possible or suspected fraud, waste, or abuse to the Department without interference, or required approval from the Vendor's management; and c. Educating Vendor staff on how to make a direct referral to the Department.	M	Yes	Standard	FDGS will work with the Department to include the proper procedures in our training and outreach curriculum. We will include how to use AuthentiCare reports and exceptions to identify possible fraud, waste and abuse. We will also include the required documentation details and contact information to provide a streamlined and direct referral process.
B5.17	Store, archive, and make accessible all records, including e-mail, involved in any litigation until the State requests the destruction, return of the records, or lifting of the litigation hold.	M	Yes	Standard	FDGS complies with administrative subpoenas and will comply with the instructions of any litigation holds as requested by the State Attorney General's Office.
B5.18	Support litigation and/or administrative hearing activities (e.g., by providing testimony, documentation), as required by the Department.	M	Yes	Standard	FDGS complies with administrative subpoenas and will support litigation and/or administrative hearing activities (e.g., by providing testimony, documentation), as required by the Department and permitted by law. Currently, we support various litigation-related activities for our other AuthentiCare clients.
PERFORMANCE					
B6.1	Vendor must comply with Affordable Care Act (ACA) Sections 1561, 1411, 1413, 1414 and 2201.	M	Yes	Standard	AuthentiCare is compliant with all relevant sections of the Affordable Care Act. However, AuthentiCare is not used for determination of benefits nor is it used for claim disposition therefore these sections are largely inapplicable.
B6.2	Vendor must comply with Section 12006 of the 21st Century Cures Act.	M	Yes	Standard	The caregiver visit data that the AuthentiCare system collects complies fully with the requirements of Section 12006 provisioned under the 21st Century Cures Act, while providing additional data collection for monitoring plan of care compliance.
B6.3	Vendor must provide applicable business intelligence information to the state.	M	Yes	Standard	Much business intelligence information is available through AuthentiCare reporting. FDGS will work with the State to define the desired metrics.
B6.4	Vendor must validate the visit procedure codes match those in the EVV record.	M	Yes	Standard	Procedure codes are associated with services setup in AuthentiCare and are matched to the visit at the time of capture.
B6.5	Vendor must validate the provider in the EVV visit record is approved for the member and matches the one in the claim / encounter submission.	M	Yes	Standard	Business rule workflows are used to assign exceptions to visits that are out of compliance. A missing provider-member relationship can be configured as a critical exception, which will prevent the visit from being submitted as a claim until the discrepancy has been addressed.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

B6.6	Vendor must validate the member is eligible to receive EVV services captured.	M	Yes	Standard	Member data includes eligibility dates and authorizations. AuthentiCare can be configured through our business rules workflow to prevent visits with ineligible members or services that have not been authorized from being sent as claims for payment. These critical exceptions must be addressed before billing is allowed to proceed.
B6.7	Vendor must validate the provider is eligible to perform EVV services captured.	M	Yes	Standard	Provider eligibility is determined by the authorization. Visits for unauthorized service are prevented from claim submission by workflows creating critical exceptions. These must be addressed before billing is allowed to proceed.
B6.8	Vendor must validate the number of units charged for a member does not exceed the members total number of approved units. The system must provide flexibility to process and flag these business rules as warnings (soft edits) or errors (hard edits).	M	Yes	Standard	AuthentiCare calculates units based on business rules aligned with the service. Business rule workflows are used to assign warnings (informational) or errors (critical) exceptions allowing the provider to address issues before visits for exhausted authorizations are submitted for billing.
B6.9	Vendor must validate the visit procedure codes are approved for the member.	M	Yes	Standard	Authorizations for services that are associated to procedure codes are used to validate that the procedures are approved for members. Configurable business rule workflows are used to create exceptions that prevent unapproved procedure codes for members from billing.
B6.10	Vendor must provide the capability to Interoperate with state systems using industry standard transactions and technology-neutral interfaces.	M	Yes	Standard	AuthentiCare supports industry standard transactions and technology neutral interface through HIPAA X12 EDI formats.
B6.11	Vendor must provide the capability to search all information including log search and playback.	M	Yes	Standard	Searching and reporting is available for easy access to both current and historical data in AuthentiCare. This includes data collected by AuthentiCare EVV and through AuthentiCare Aggregator. For example visits can be searched by many data points including service date, service, member, worker, and/or provider. Report search criteria is available in a similar fashion.
B6.12	Vendor must provide authorized stakeholders uniform access to information.	M	Yes	Standard	Stakeholders are provisioned accounts into AuthentiCare web for uniform access to data. Each user is assigned to a role that fits their business need. Roles are assigned rights that control the information available.
B6.13	Vendor must provide Role-based access control to all system features and data, including specified data elements.	M	Yes	Standard	AuthentiCare supports configurable roles and rights. Each role is assigned specific rights to control what features and data are available. This, along with our mature data scoping, allows user access to only data with which they are associated. For example, one provider agency cannot access another agency's visits.
B6.14	Vendor must provide Multi-Factor Authentication.	M	Yes	Standard	Multi-Factor Authentication (MFA) into AuthentiCare web is provided via username/password (something you know) and a time-managed One Time Pin (OTP) sent through email (something you have). The OTP is sent to the email on file for the user through our enterprise PingFederate solution. For mobile users, MFA is established using username/password (something you know) and a device ID on file in AuthentiCare (something you have).
B6.15	Vendor must provide interoperability with the DHMS claims adjudication process.	M	Yes	Standard	AuthentiCare is interoperable with claim adjudication processes through the exchange of HIPAA X12 EDI 837 claims, 835 remittance for payments and denials and 999 for acceptance and rejection.
B6.16	Vendor must validate incoming data based on data standards and configurable business rules.	M	Yes	Standard	Data is validated while entered and accepted using formatting and confirmation against data on file following standards and configurable business rules.
B6.17	Vendor must provide the capability to save and transmit data regardless of the mode of communication.	M	Yes	Standard	Data received into AuthentiCare is saved and can be transmitted based on requirements. This is regardless of transmission method which could be through our mobile apps, IVR, secure file transfer, API or web upload.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

B6.18	Vendor must provide conceptual and logical data models for all EVV data entities including: • Benefits • Claims • Encounters • Service/care plan • Physicians order • Services • Visits • Verifications • Log/Audit trail • Payments • Accounts	M	Yes	Standard	FDGS will provide information on EVV data models available while protecting our intellectual property that could pose a security risk to our other customers.
B6.19	Vendor must provide capability to display data in a variety of industry standard formats.	M	Yes	Standard	AuthentiCare reporting allows the selection of industry standard formats such as PDF, Excel, CSV, and XML.
B6.20	Vendor must preserve and make available all data and records to the state.	M	Yes	Standard	FDGS will make available all data to the state based on the legal and contractual retention requirements.
B6.21	Vendor must provide all state-centric data rights to the state.	M	Yes	Standard	FDGS operates from the position that the State owns the EVV data.
B6.22	Vendor must verify the date, time the service begins and ends, and location of services captured.	M	Yes	Standard	EVV captured in AuthentiCare includes the date and time service begins and ends, as well as the location of service as established in the 21st Century Cures Act. This information is stored directly from the mobile apps based on data gathered from the mobile device such as time and location or using the server date and time or Automated Number Identification (ANI) collected from the toll free calls into our IVR.
B6.23	Vendor must provide EVV data flows and interfaces to state identified systems.	M	Yes	Standard	AuthentiCare provides data exports and direct interfaces to state systems today. We have included high-level data flows as part of Attachment 3 - Environments, Architecture and Data Flows. FDGS will provide expanded EVV data flows and interface specifications into state identified systems such as the MMIS and data warehouse/EBI based on documentation and connectivity to these systems provided by the State during our implementation project.
B6.24	Vendor must provide CMS MITA Framework alignment information regarding the EVV solution.	M	Yes	Standard	FDGS satisfies MITA's Modularity Standard by employing a modular, flexible approach to systems development, including the use of open interfaces and exposed application programming interfaces (APIs) to separate business rules from core programming. In support of the MITA Industry Standards condition, integration capabilities are based entirely on open-systems standards and accommodate communications to database management systems and back-end solutions.
B6.25	Vendor must provide standardized business rules definitions in human and machine-readable formats.	M	Yes	Standard	Business rules definitions are available in human and machine readable formats.
B6.26	Vendor must adhere to HL7 standards.	M	Yes	Standard	Today, AuthentiCare provides real-time delivery of client service visit information via web service interface and APIs. XML-based APIs are available for data exchange with MCOs, provider agencies and state systems. HIPAA EDI X12 formats are used to exchange claim, remittance and authorization information. We will work with DHHS to review its EDI companion guide and verify that the appropriate HL7 standard is met for data exchange and interoperability. Interfaces are provided using multiple delivery methods: • Transactional secure JSON/REST web services • File upload and download to and from the secure AuthentiCare web • File upload and download to and using SFTP
B6.27	Vendor must comply with applicable Federal and State of New Hampshire Policies and Procedures.	M	Yes	Standard	FDGS will comply with applicable Federal and State of New Hampshire policies and procedures.
B6.28	Vendor must provide data aggregation services.	M	Yes	Standard	AuthentiCare Aggregator successfully used in other states is offered as part of our solution for DHHS.

RFP-2022-DLTSS-05-ELECT-01 #2022-031

First Data Government Solutions, Limited Partnership

Exhibit G, Attachment 1, EVV Business and Technical Requirements

Contractor Initials: *SM* Page 13
Date: 9/2/2022

Exhibit G, Attachment 1
EVV Business and Technical Requirements

86.29	Vendor must provide Role-based user experiences that optimize Effort to Perform; Efficiency, Timeliness of Process and User Satisfaction metrics.	M	Yes	Standard	AuthentiCare supports Role-Based configuration to allow users to have rights to read, edit and/or create depending on user's role. FDGS works with stakeholder groups during the implementation phase to determine the role and associated rights that best suits their job function. User Satisfaction metrics are pulled from multiple sources, for example training sessions, Call Center email/phone, and mobile app ratings/reviews.
86.30	Vendor must provide configurable system alerts and notifications.	M	Yes	Standard	AuthentiCare supports configurable alerts and notifications. For example, late and missed visit notifications can be configured to allow providers to send a substitute worker in the event the assigned worker does not arrive. Thresholds for late and missed visits are configurable as is the escalation of alerting.
86.31	Vendor must provide support for multiple DHHS programs and services including those covered by the state plan, waivers, Home Healthcare and Personal Care.	M	Yes	Standard	AuthentiCare supports multiple programs in ten states including fee-for-service and MCO models along with multiple waivers, Home Healthcare and Personal Care. For example, AuthentiCare supports supports 3 MCOs in New Mexico and 4 MCOs in Nevada. In Kansas, Oklahoma and South Carolina both Personal Care and Home Healthcare services are collected. AuthentiCare communicates with MMIS systems, MCO systems, and claim clearing houses.
86.32	Vendor must support ability to capture stakeholder satisfaction through multiple ways (e.g., surveys, operational metrics from usage in production).	M	Yes	Standard	FDGS supports the ability to capture stakeholder satisfaction through training surveys, operational metrics, call center email and phone call auditing, and mobile app reviews and ratings.
86.33	Vendor must provide standardized EVV data elements and definitions as approved by the state.	M	Yes	Standard	AuthentiCare is configurable to use State terminology within the web site and mobile app. Some examples include clock in/out vs. check in/out, claims vs. visits, workers vs. service attendants vs. caregivers, and members vs. clients.
86.34	Vendor must have the capability to validate the visit units against different frequency types (daily, weekly, monthly) as approved by the source system.	M	Yes	Standard	In AuthentiCare, authorizations are set for different service periods including daily, weekly and monthly as received from the source system.
86.35	Vendor will conform with all relevant federal requirements, or be in conformance no longer than a six month period after passage of rule changes. All federal requirements changes must be completed at no cost to the Department.	M	Yes	Standard	Our CMS Certification SMEs continually monitor federal regulations and requirements to identify potential impacts to AuthentiCare and EVV program and policy. Many times, changes at the federal level are analyzed and incorporated into AuthentiCare for all clients as part of our product enhancements with no additional cost to our clients. Unique changes to New Hampshire EVV program or policy will be evaluated through the Change Management process. We will examine any need for specific changes in New Hampshire to take advantage of the 1,500 annual support hours before any potential cost to the Department.
86.36	Vendor will cooperate with and assist the Department in responding to all open records, law enforcement, federal and State audit, and review requests. Vendor shall provide audit support (e.g., random sample generation, data extracts, hard-copy documents), and provide any requested data or information within Department approved timeframes.	M	Yes	Standard	FDGS will comply with applicable Federal and State of New Hampshire public records or information requests, and has a policy in place in order to comply with such requests in a timely fashion.
PRIVACY AND SECURITY					
87.1	Vendor must ensure that all personnel and vendors entering an individuals home for maintenance/repair/replacement of an EVV device have satisfied the background check requirements set forth in state Code. Vendor will maintain copies of background checks for all staff entering an individuals home for maintenance/repair/ replacement of EVV devices and provide the background checks to state upon request.	O	Yes	Standard	All FDGS/Fiserv employees must satisfy background check requirements prior to employment. However, FDGS is not proposing to provide services that would require onsite support in individual's homes, therefore this requirement does not apply.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

B7.2	Vendor must maintain a record (audit trail) for any manual verifications. For each manual verification the EVV will store the information entered the person entering the information the billing provider the direct care worker the individual receiving services the date and time of the visit the reason for the manual verification and the date and time of the manual verification.	M	Yes	Standard	AuthentiCare maintains a complete audit trail for manual data entry including who made the entry and the date and time as well as a record of the previous state of the data. This includes visits manually created and electronically-created visits that have been modified manually. Reason for manual entry can be required by configuration through reason codes and/or free-text note entry.
B7.3	Vendor must offer a variety of methods by which the direct care worker member and/or their responsible party may indicate that a visit validated including but not limited to electronic signature voice recognition or other biometrics. All use of electronic signatures must meet the requirements set forth in state rules and guidance.	M	Yes	Standard	AuthentiCare offers member or responsible party attestation through electronic signatures in our mobile app and voice acknowledgement through our IVR system. Direct Care Workers validate their visits through the check-in and check-out process on mobile and IVR. FDGS agrees to meet State requirements for electronic signatures.
B7.4	Vendor's BCDRP must address short- and long-term restoration relocation or replacement of resources necessary to ensure the smooth continuation of operations related to state data. Such resources may include among others communications supplies transportation space power and environmental controls documentation people data software and hardware. Vendor must have documented disaster recovery plans that address the recovery of lost State data as well as their own. Systems must be architected to meet the defined recovery needs.	M	Yes	Standard	FDGS has documented Business Continuity and Disaster Recovery Plans. These are tested annually with Disaster Recovery processing live activity for several days to a week at our secondary data center. Data is replicated in real time between our geographically diverse data centers in Chandler AZ and Omaha NE. Each data center has full staffing and redundant environmental and power systems in addition to duplicate servers for full capacity. Within each data center multiple servers are load balanced to limit the impact created by a failure in any one server or piece of hardware. Our Business Continuity Plan specifies critical business functions and systems and documents the plan should those become unavailable. The biggest test of BCP has been the COVID pandemic where FDGS staff were immediately able to work from home when leadership deemed it not safe to work in the office. Recovery Time Objective and Recovery Point Objective are documented. Database backups are taken and distributed across our data centers so they do not leave our facilities but are stored across geography. Full backups are taken nightly with iterative backups completed throughout the day. This coupled with the database replication minimizes the risk of data loss.
B7.5	Vendor shall provide a Continuity of Operations Planning (COOP) that addresses emergency operations and response planning of EVV for the business as well as their own. Systems shall be architected to meet the defined business operational needs.	M	Yes	Standard	FDGS has a documented Business Continuity Plan that covers COOP, and this can be shared with the State in a secure manner. Our Business Continuity Plan is reviewed and tested annually.
B7.6	Vendor shall provide a detailed System Security Plan (SSP). Plan shall be architected to meet the defined requirements of the Department's Information Security Office. Plan should support key security management activities before and after system authorization.	M	Yes	Standard	FDGS has developed and maintains an industry leading standard EVV System Security Plan (SSP) that serves our existing clients. FDGS will develop the Security Status Report based on our SSP and active monitoring of New Hampshire AuthentiCare system components and provide to DHHS annually. We will examine NIST 800-53 rev 4 for additional guidance for the Security Audit Report. We maintain a documented security plan that is regularly audited by the FFIEC, our Payment Card Industry (PCI) assessor, and under SSAE 18 by Deloitte and Touche. Fiserv/FDGS security plans and procedures are prepared at a facility level, where the AuthentiCare solution is hosted in large scale, redundant data centers. The AuthentiCare platform is independently audited each year to produce an SSAE 18/SOC 2 Type 2 report. The report covers confidentiality, integrity and availability controls. Due to the sensitive nature of AuthentiCare's annual SSAE 18/SOC 2 Type 2 report, FDGS agrees to provide a shareable version upon request from DHHS.
B7.7	Vendor shall establish a user friendly IT Issue Tracking System.	M	Yes	Standard	The FDGS Client Services incident management process uses the ServiceNow tracking and reporting tool.
B7.8	Vendor shall provide an IT Issue Tracking Plan/Guide	M	Yes	Standard	FDGS will provide our IT Issue Tracking Plan including our prioritization definitions and escalation procedures.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

67.9	Vendor must support the encoding of data for security purposes (encryption at rest) and for the ability to access the data in a decrypted format from required tools for authorized users.	M	Yes	Standard	PII and PHI data at rest in AuthenticCare databases is column-level encrypted using Voltage, an API based tool. Access to data in its decrypted format is only available to authorized users through the AuthenticCare application and is not accessible natively in our databases. Files at rest are also encrypted using Voltage. Access to data that has been encrypted is only available through logged application interfaces.
SYSTEM EFFICIENCY					
68.1	Vendor must provide an intuitive user interface/device interaction that is minimally burdensome for the direct care workers and members.	M	Yes	Standard	Worker interfaces into AuthenticCare are designed to be minimally burdensome based on the goal of maximizing the time spent providing service to members. A few taps on the mobile app after logging in and the worker has checked in or out. IVR interactions in many cases are less than one minute dependent on the complexity of the associated business rules. The AuthenticCare web site is an easy to use system for members and their representatives to review and approve visits for claim submission.
68.2	Vendor must provide the ability for the member and/or their authorized representative to act on behalf of the member, to include, delegation of visit verification responsibility to another person of suitable age and discretion. The system must allow multiple individuals to be designated and must track additions and deletions. Changes should be able to be made easily via the member's portal.	M	Yes	Standard	AuthenticCare supports a representative role and functionality for self-directed care that allows the member or their representative to review and approve visits for submission for payment. Multiple representatives can be assigned to a member.
68.3	Vendor must provide their solution approach to handle when the Direct Care Worker (DCW) and the authorized representative are the same person.	M	Yes	Standard	In AuthenticCare workers and representatives are defined separately and the system allows for a DCW to also serve as an authorized representative. When performing caregiver duties, the DCW uses the AuthenticCare IVR or mobile app to check in and check out for visits. When acting as an authorized representative, the individual logs into the AuthenticCare web portal to complete tasks such as reviewing and/or approving visits. We will work with DHHS to understand program rules for DCWs that dually serve as authorized representatives.
68.4	Vendor must support quick and efficient way to support modifications of the visit data by the member/Authorized Representative without compromising the original record.	M	Yes	Standard	A full audit trail is maintained for changes to visits recording the original state of the visits data along with the date and time of the change and the account that made the change. Free-text notes and reason codes can also be recorded to document the reason for the change.
68.5	Vendor must generate reports to monitor and track retention rates at for the DCW. The reports should provide flexibility to look retention rates at the State level or individual provider agency/MCO level. The reports should compare with established state/regional/national standards.	M	Yes	Standard	AuthenticCare stores effective employment dates and worker status for DCWs. Data is made available to authorized users within the standard reporting suite. For example, our Worker by Provider report includes Worker ID, Name, Start Date, Termination Date and all services assigned in their worker profile. Data is grouped by provider agency and can be filtered down to a specific provider agency, worker, worker status and/or service. Data scoping based on user roles allows for State users to see data for all DCWs and provider agencies in the EVV system. MCO users only see workers who deliver service to their members and provider agency users only see their own employees. FDGS will work with the State to provide reporting on retention rates and the sources of data for the desired established standards.
68.6	Vendor must provide a flexible solution to support for circumstances where a visit starts and/or ends away from the member's place of residence.	M	Yes	Standard	AuthenticCare mobile apps and IVR capture visits regardless of location. Visits beginning in one location and ending in another are supported. The system supports multiple locations of record for members, and visits can take place in the home or community.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

B8.7	Vendor must provide a scheduling module to reduce member provider agencies and direct care worker/staff burden.	M	Yes	Standard	<p>AuthentiCare's scheduling module makes worker check in even faster, reducing burden on workers. The module also facilitates late and missed visit reporting and alerts, driving better service for members.</p> <p>In AuthentiCare a scheduled visit is called an event. Events can only be created for authorized client/service/provider/caregiver combinations. The scheduling feature accommodates scheduling of both primary and back-up caregivers for each event.</p> <p>AuthentiCare tracks the number of service units available for scheduling events and notifies the scheduler through an alert if an event exceeds the total number of units available. Providers can discard, accept or change events from the event acknowledgement page.</p> <p>If a caregiver is scheduled for an event on a regularly occurring day off as noted on the Worker Entity Settings page, AuthentiCare displays a warning message for this conflict. The scheduler may choose to change the event or to save it even though a conflict exists. AuthentiCare's scheduled warnings are meant to assist schedulers, but not to prevent the scheduler from creating an event if a conflict is detected.</p>
B8.8	Vendor must provide a flexible and user configurable reporting tool which shall not only include a library of standard reports but also support the development of ad hoc reports in accordance with the user role designation.	M	Yes	Standard	<p>AuthentiCare's robust reporting engine provides a tool for easily customized EVV program monitoring and management, which helps identify and reduce fraud, waste and abuse. AuthentiCare contains a broad spectrum of on-demand reports with ad hoc functions like drop-down list filters, parameters, date ranges and other selections that allow users to report the data of which they are specifically interested.</p> <p>Our reporting tool gives stakeholders the ability to search through both summary and detailed data views. Using selection criteria for each report, a user can easily customize the standard report to meet specific requirements and run a one-time report, save a report template that they want to run regularly for ongoing analysis or metrics submissions.</p> <p>These reports provide stakeholders, as well as the provider community (based on their security access authority), views into the electronic visit and verification data to manage the programs, confirm members receive needed care and help identify fraud, waste and abuse.</p>
B8.9	Vendor must include functionality that allows the State to conduct surveys including member /provider/ state staff satisfaction surveys. The data collected through the surveys will be made available in the reporting system.	M	Yes	Standard	FDGS uses a third-party, Commercial Off The Shelf (COTS) survey module allowing the State to conduct surveys of members, providers and state staff. Guidance for use of the tool and reporting on survey data collected will be made available to the State.
B8.10	Vendor must have the flexibility for members and/or their authorized representative party to make changes to their individual preferences in the system to receive alerts and notifications.	M	Yes	Standard	Members or their representatives can make changes to their alert and notification preferences through the AuthentiCare web portal.
B8.11	Vendor must describe their approach and process for device management and the process for notification, recovery and or reinstallation of the device in case it is reported stolen or member relocates or leaves the program.	O	Yes	Standard	In the event that a worker's mobile device is lost or stolen, it can be disabled in AuthentiCare and their new device enrolled. If a member leaves the program, the device can be disabled following the same process. Note that the limited data on the mobile device is encrypted.
B8.12	Vendor must ensure that the device firmware and version is up to date and updates are not disruptive to the user experience.	O	Yes	Standard	FDGS publishes minimum device requirements including the operating system (OS). Updates to the apps are managed through the related app store. Understanding the challenges for workers to upgrade their devices, FDGS limits the sunset of support of devices. Historically updates to devices have only been mandated when security vulnerabilities require it. FDGS communicates when new releases are available and when devices will no longer be supported in advance to allow workers to prepare.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

B8.13	Vendor must ensure that there are adequate software and process controls in place to ensure all personal information is removed in case the devices are to be reused.	O	Yes	Standard	The minimal data stored on mobile devices is encrypted and only accessible through the specific worker's login. When the mobile device has a connection to the internet or cellular network, the visit is saved to AuthentiCare in real-time. However, when there is no Wi-Fi or cellular data coverage at the time and location of service delivery, the AuthentiCare mobile apps record time and satellite-based GPS location to allow caregivers to create visits the same as when they are online. Visit data captured offline is encrypted and stored on the device. When a connection is restored the visit details are forwarded to the AuthentiCare servers and removed from the device (Store and Forward).
B8.14	Vendor must provide the approach to device upgrades and ensure it is not disruptive to the user.	O	Yes	Standard	In a standard AuthentiCare implementation, workers bring their own device (BYOD) or providers supply them as assigned to an individual worker. When devices are to be upgraded, the new device ID is assigned to the worker in AuthentiCare and the worker proceeds without interruption.
B8.15	Vendor must provide details of their help desk processes and how will the effectiveness of technical support be monitored and reported by stakeholder (member/caregiver/State).	M	Yes	Standard	Initial contact into our help desk occurs in our call center. Call center agents open incident tickets in our ServiceNow tracking system. The agent will provide the incident (INC) number to the caller and will work with them to resolve most issues. For issues that cannot be resolved in the initial contact, the INC is escalated into our Tier 2 support team. Our advanced technicians in Tier 2 further work the INC and communicate with the requestor. Issues not resolved in Tier 2 are escalated to our Tier 3 system experts that includes senior product and development personnel for resolution. Each step in this process is documented in ServiceNow for reporting and knowledgebase purposes. Trends in requests are reviewed to identify process improvements. Our monthly scorecard includes data on inquiries and escalations over the previous six months into our support organization as well as the top 5 inquiry categories. Also included is a ticket creation history showing the number of tickets per month, top ticket categories, severity, and length of time tickets have been open. In addition call center metrics are included for total calls, average handle time, average speed of answer, abandon rate, and percentage of calls answered within 30 seconds.
B8.16	Vendor must provide help desk support for all stakeholders (member/caregiver/MCO/State).	M	Yes	Standard	Help desk support is available to all users of AuthentiCare. Typically workers and members first contact their provider agencies with the help desk acting as an escalation point.
B8.17	RESERVED				Not Applicable
B8.18	RESERVED				Not Applicable
B8.19	Vendor must ensure that the staff entering an individual's home for maintenance/repair/replacement of EVV devices will be bonded and insured.	O	Yes	Standard	FDGS does not propose to have staff entering individual's homes, therefore this requirement does not apply.
B8.20	Vendor must provide the ability to support Pilot Roll out of the EVV system (by area, program, by provider group) to verify and validate the user experience and take feedback from the Pilot roll out to make required changes to improve user adoption and satisfaction.	M	Yes	Standard	Most of our AuthentiCare implementations began with a pilot period so our team is very familiar with this process. FDGS will work with the State to determine the appropriate groups and areas to pilot initial and early use of AuthentiCare for EVV.
B8.21	Vendor must provide system and associated process control to ensure that all issues are acknowledged, tracked, managed and resolved to ensure user satisfaction.	M	Yes	Standard	FDGS support procedures require tickets to be open for all client requests for service. Dashboards built within our ServiceNow system are used to track time to resolve, bring attention to issues with multiple reports, and provide support leadership visibility into those that are aging and confirmation of timely resolution. FDGS understands and shares the expectation for prompt issue resolution.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

B8.22	Vendor must document the transition strategy from the alternative device/method as technology changes and/or GPS technology becomes more widely available in the State.	M	Yes	Standard	FDGS proposes to use our mobile apps as the primary capture method in New Hampshire so alternative devices and methods are not required. The apps use the satellite based technology available in today's devices so there is no dependency on Wi-Fi or cellular connectivity to capture GPS at the time of the visits. In extremely rare instances where GPS is not available, our IVR is available to capture EVV via toll free call. For over 73 million mobile check ins and check outs across of our statewide implementations, over 99.6% captured GPS coordinates. Less than 100 total members across ten states receiving a mobile visit have not had GPS captured with nearly all of these logging less than three attempts.
B8.23	Vendor must have the ability to interface with providers existing payroll systems for the purpose of sharing validated visit data in order to populate care workers timesheets for payroll purposes. The use of this functionality by providers is optional and as such it is the providers sole responsibility to pay any costs associated with the building of the interface.	O	Yes	Standard	Many providers use our Claim Data Listing or Time and Attendance Report in CSV format to exchange EVV data with their existing systems. Should they desire additional interfaces, FDGS will establish a process with the State in support of provider paid integration.
B8.24	Vendor must provide alternate solutions to manage retroactive Service Plan and authorization changes for specific services and/or programs.	M	Yes	Standard	AuthentiCare automatically connects authorization updates to non-billed visits. For example visits may be recorded prior to receipt of authorization in AuthentiCare. The visit will be held with a critical exception until the authorization has been received. This prevents rework for providers and the payment system as unauthorized claims are most often denied. Once the authorization has been received our workflow process will automatically connect it to any related visits which can then be exported for payment.
B8.25	Vendor must provide for manual verification if needed and allow for providers to attest to the presence of hard copy documentation for any manual visit verification.	M	Yes	Standard	AuthentiCare supports manual entry through the web site and can require notes for the provider to attest to the presence of hard copy documentation.
B8.26	Vendor must be capable of collecting and storing data offline during any downtime such as regularly scheduled maintenance.	M	Yes	Standard	AuthentiCare Mobile stores data encrypted in the mobile device while off line or if the system is unavailable. Data from mobile and IVR is written to recoverable queues and will be processed once the system is again available. Our redundant server environment allows for individual servers to be taken offline for maintenance without taking the entire system down, reducing time that AuthentiCare is not available during maintenance.
B8.27	Vendor must develop and operationalize a communication plan that will be used to ensure all impacted parties (e.g. individuals receiving services, direct care workers, providers) are knowledgeable about planned maintenance and updates.	M	Yes	Standard	As a standard part of our State implementations, FDGS creates a Customer Care Plan which includes a communications plan capturing methods, frequency and standard templates. FDGS will work with DHHS to identify stakeholders groups and the types of communication that each should receive.
B8.28	Vendor must allow for a flexible roles based access and allow the State to designate entities to assign roles (e.g. a provider agency will assign roles to direct care workers and a case management agency will assign roles to individual case managers).	M	Yes	Standard	AuthentiCare supports flexible roles based access. Designated admins from the State and provider communities can create user accounts and assign roles as appropriate to their own roles and access.
B8.29	The vendor solution must provide an intuitive user interface that minimizes data entry, verifies entered data values against specified data type and format and avoids duplicate entry of same information.	M	Yes	Standard	Interfaces to State, MCO, and Provider systems reduce the need for manual data entry into AuthentiCare. For data that requires manual entry our easy to use web portal is available. Regardless of manner of data entry, validation rules are in place to confirm valid data has been provided and not duplicated.
B8.30	The vendor must system allows for search and easy access to both current and historic data in the system (e.g. days worked, start time, finish time, total hours, etc.).	M	Yes	Standard	Searching and reporting is available for easy access to both current and historical data in AuthentiCare. This includes data collected by AuthentiCare EVV and through AuthentiCare Aggregator. For example visits can be searched by many data points including service date, service, member, worker, and/or provider. Report search criteria is available in a similar fashion.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

B8.31	The vendor must create all reports and provide a real-time performance monitoring dashboard to support the Key Performance Measures, it can exclude Department approved planned downtime (i.e., system unavailable for use).	M	Yes	Standard	<p>Real-time application performance monitoring of the AuthentiCare components uses AppDynamics Performance Monitor (APM), a suite of tools to maintain stability and availability of the AuthentiCare solution platform. APM also allows FDGS to monitor, in real time, the performance of the key business functions of AuthentiCare within the hardware and software infrastructure layers.</p> <p>Based on monitoring results, APM creates alerts on critical resources component utilization or when response thresholds are exceeded so that proper action can take place to restore normal functioning and performance of the systems. Unplanned outages or performance issues are communicated to the Department as well.</p> <p>Log data are collected in a central logging platform and fed into our Joint Security Operations Center (JSOC) toolset for monitoring and alerting, which is staffed 24/7. Review of audit logs are configured through Splunk to meet these monitoring requirements for unauthorized access and ongoing reporting of events.</p> <p>FDGS will update our Monthly Scorecard to include reporting details for all approved Key Performance Measures.</p>
SELF-DIRECTION					
B9.1	The Vendor's EVV System shall have the ability to interface with all provider systems. The Contractor shall work with the State and the providers in defining the elements to be included in the interface but shall, at a minimum, include details of all visits for members using self-directed services.	M	Yes	Standard	FDGS is experienced in exchanging data with FMS providers in support of self directed care in multiple states. We will work with the State to determine the best suited interface.
B9.2	The Vendor's EVV System scheduling module shall be accessible to members/authorized representative and providers, allowing providers and members including, but not limited to, members who use a self-directed option, to use the EVV System to schedule DSP visits. The Contractor's scheduling model shall permit flexibility in scheduling visits (e.g., adjusting scheduled service visit start times) and be designed to reduce member, provider agencies and DSP/staff burden.	M	Yes	Standard	<p>AuthentiCare's scheduling module can be assigned to roles for members and their representatives along with their providers to establish visit plans. Scheduling supports daily, weekly, and monthly visits and recurring schedules can be created.</p> <p>Recurring visits can be scheduled by every number of days or weekdays and set to end on a specific date or after a specified number of visits. The weekly configuration supports the number of weeks between visits as well as the day of the week and can be configured to end after a number of visits or on a specific date. Monthly schedules can be configured for specific days of the month and how many months in between visits, of the first, second, third, fourth or fifth given day and how many months between visits.</p>
COMMUNICATION PLAN AND USER TRAINING					
B10.1	The Vendor must develop and maintain a communication plan in order to facilitate the effective and efficient communications across the project team. This includes stakeholders, business partners and the public if this is a public facing application. The plan, which is subject to State review and approval, must comprehensively identify the Vendor's outreach and education strategies throughout the EVV Project implementation and term of the Contract.	M	Yes	Standard	<p>The Communications Plan is a standard project deliverable communicating the formal communications approach, processes, methods, formats and templates, stakeholders, roles and responsibilities. Additionally, our Training Plan includes a comprehensive training communication strategy, which details ongoing methods of communication and support with the State, providers and other key stakeholders; including live Support Forums, Learning Management System links for on-demand options, training ticket management, and communication of survey and training participation feedback.</p> <p>The Communications Plan, along with the Training and outreach plans, indicates the strategy for formal communication with all parties, both internal and external over the term of the contract. Issues resolution is included under the Risk and Issue Management sub-plan. This Customer Care plan will be reviewed annually with DHHS.</p>

Exhibit G, Attachment 1
EVV Business and Technical Requirements

B10.2	The Vendor's Communication Plan must address the outreach and communications to stakeholders, including DHHS and its State partners, contracted MCOs, members/families, providers, DCWs and other interested parties. The Contractor's Communication Plan must cover: <ul style="list-style-type: none"> • Key planned stakeholder communications through the program development and implementation; • System user education related to the purpose and use of EVV System • Issue Resolution Process • Availability of Online and Telephonic User Support. • Notifications to users of System downtime due to System updates and scheduled maintenance • Identification of roles and tools for members, providers, MCOs and the State to use to supplement member and stakeholder educational activities performed by the Contractor. 	M	Yes	Standard	The Communications Plan is a standard project deliverable communicating the formal communications approach, processes, formats, methods, stakeholders, roles and responsibilities. It also details planned communication strategies for stakeholder outreach, ticket/issue resolution and how scheduled system downtime will be communicated. User telephony and on-line support are included under the Customer Care or Operations Management sub-plan. The Training Plan will include a detailed list of all training types and audiences, along with how frequently they will be offered and what methodology will be used. All training sessions include sharing direct contact information for the assigned trainer plus all other available support options for that audience. In addition, the Communications Plan, along with the Training and outreach plans, indicates the strategy for formal communication with all parties, both internal project stakeholders as well as external agencies and vendors over the term of the contract. The comprehensive Customer Care Plan, including the Communication Plan, will be reviewed on a yearly cadence.
B10.3	The Vendor's Communication Plan must include the key message, targeted audience for the communication, the communication method(s) or format(s) to be used, and the timing and frequency of the communication.	M	Yes	Standard	Our Customer Care Plan includes the Communication Plan detailing communication methods, formats, frequency and timing. Additionally, The Training Plan comprehensively details the cadence at which we plan to meet with key stakeholders, including multiple weekly meetings with different audiences and live monthly or bi-monthly Support Forums.
B10.4	The Vendor must work with the State on "branding" the EVV System (including a logo) and utilize the DHHS website where all communication and educational tools and other pertinent EVV information will be posted.	M	Yes	Standard	Each State's AuthenticCare website is branded with the State's name and logo of choice. For example, some states choose to use their State seal to brand their web portal. Within the AuthenticCare website users can access training materials and announcements, and links to State websites that have information pertinent to EVV. Fiserv will work with the State to create a banner for the AuthenticCare web portal that best represents New Hampshire DHHS and to determine the contents of the learning and communication repository.
B10.5	Vendor must submit a detailed Training Plan that, at a minimum, addresses the following: a. Summary of training approach that focuses on the train-the-trainer methodology, objectives, and desired outcomes. b. Training needs analysis, including an assessment of the target audience and their knowledge and skills. c. Recommendations on type and delivery approach based on training needs analysis. Mode of Training (Web, In Person). d. Summary of proposed training materials and documentation in addition to hands-on training. e. Approach to maintaining training documentation and accompanying materials. f. Approach to providing training necessary to support new functionality and/or major software releases that materially change the user interaction. g. Approach to processing for incorporating feedback to improve train the trainer effectiveness over the course of the Contract. h. Training Schedule for each stakeholder type (provider/caregiver, member, state, other). i. Log, Collect and Report on the effectiveness of the training sessions.	M	Yes	Standard	AuthenticCare's Training team provides a customized Training Plan for each state, which includes: a. Desired outcomes for all audiences utilizing a combination of train-the-trainer (T3) and direct instruction approaches. b. Needs analysis based on State-specific requirements and assessment of target audiences. c. Training approach that utilizes mixed modalities, including both synchronous and on-demand options through Instructor Led Training (ILT), Virtual ILT, and our Learning Management System, which includes a video library. d. Samples of ad hoc training options and delivery methods. e. Examples of how we version and index our training documentation. f. Continuing education/change management training g. Plan also includes survey information, which is collected from training participants and used to inform subsequent training sessions and approaches. h. Training schedule is provided to the State, which includes descriptions, links, historic recordings and audience descriptions for all session types. i. Reporting is pulled weekly, unless specifically requested by the state, including both participation logs and survey reports. These are communicated to the State evaluate attendance, knowledge and training effectiveness.
CMS CERTIFICATION					
B11.1	The Vendor must work and assist DHHS to develop of Key Performance Indicators (KPIs).	M	Yes	Standard	AuthenticCare's CMS Subject Matter Expert (SME) will consult with the State to calculate KPIs that meet the State's requirements for CMS, and to establish a repeatable approach for delivering CMS OBC quarterly KPIs. Experience supporting our other clients through this process will be of benefit DHHS.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

B11.2	The Vendor shall lead the effort to achieve CMS certification of the system with involvement of DHHS and Quality Assurance Contractor staff. Activities include compliance with outcome statements, evaluation criteria, development of Key Performance Indicators (KPIs), other certification requirements as described in CMS guidance or required by DHHS.	M	Yes	Standard	Our approach to CMS Certification for DHHS will be through active participation during all phases of the project from DDI to post-go-live. Additionally, the CMS Certification SME will lead the activities required for formal CMS certification. FDGS understands the certification guidance and requirements based on our regular communication with CMS and our hands-on project experience, and will collaborate with DHHS and Quality Assurance Contractor staff to gather all required evidence for ORR. We will continue working with DHHS and CMS through delivery of Key Performance Indicator reports and in preparation for the final certification review meeting.
B11.3	The Vendor shall work with the Department to conduct a CMS Operational Readiness Review prior to go-live.	M	Yes	Standard	FDGS will work with DHHS and other relevant stakeholders to conduct a successful CMS Operational Readiness Review within the timeframe required to complete Certification. FDGS has assisted four other states in completing their ORRs and has created effective tools and methodologies for the entire certification process.
KEY PERFORMANCE MEASURES					
B12.1	Vendor's solution shall be available twenty-four (24) hours a day, 7 days a week except for during scheduled maintenance. Vendor shall ensure that the solution is available ninety-nine percent (99%) of the time as measured on a monthly basis and that downtime is no greater than twenty-four (24) hours per incident. Vendor shall provide five (5) business days' notice to the State prior to its regularly scheduled maintenance windows. Availability is calculated monthly as follows: Availability percentage = unplanned downtime (Total downtime minus approved downtime) divided by Total time (24x7).	M	Yes	Standard	FDGS agrees that AuthentiCare will be available 24/7 other than scheduled maintenance at a minimum of 99% of the time on a monthly basis with downtime no greater than 24 hours per incident. Our SaaS offering uses multiple load-balanced servers for presentation and application along with database clusters designed to maximize system availability. Our secondary data center provides full capacity in the event the primary facility is not available. FDGS will notify DHHS of regularly scheduled maintenance windows.
B12.2	Provide real-time performance monitoring dashboard availability ninety-nine percent (99%) of the time, twenty-four (24) hours a day, seven (7) days a week, excluding Department approved planned downtime (i.e., system unavailable for use). Availability is calculated monthly as follows: Availability percentage = unplanned downtime (Total downtime minus approved downtime) divided by total time (24x7).	M	Yes	Standard	Real-time application performance monitoring of the AuthentiCare components uses AppDynamics Performance Monitor (APM), a suite of tools to maintain stability and availability of the AuthentiCare solution platform. APM also allows FDGS to monitor, in real time, the performance of the key business functions of AuthentiCare within the hardware and software infrastructure layers. Based on 24/7 monitoring results, APM creates automated alerts on critical resources component utilization or when response thresholds are exceeded so that proper action can take place to restore normal functioning and performance of the systems. Unplanned outages or performance issues are communicated to the Department as well. Log data are collected in a central logging platform and fed into our Joint Security Operations Center (JSOC) toolset for monitoring and alerting, which is staffed 24/7. Review of audit logs are configured through Splunk to meet these monitoring requirements for unauthorized access and ongoing reporting of events. FDGS will update our Monthly Scorecard to include reporting details for all approved Key Performance Measures.
B12.3	Request approval from the Department prior to scheduling non-emergency system downtime or maintenance during hours of operation no later than five (5) Business Days prior to downtime.	M	Yes	Standard	FDGS will notify the Department of non-emergency maintenance a minimum of 5 business days prior. FDGS will provide our maintenance calendar early in our engagement.
B12.4	Provide a user interface response time of less than two (2) seconds per discrete transaction. Response time is measured from the time the data packets leave the State network to the time a response is received from the Contractor's software application.	M	Yes	Standard	AuthentiCare response time will be less than two seconds in return to our edge web servers. The speed of the internet between our perimeter and the State's network is no in our control.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

B12.5	Vendor must ensure that the Data integrity error rate and routing errors of any transaction is less than .001%. Transactions include all EVV data activity within or interfaced with the Vendor's system. Data cannot be modified undetectably. In addition, data needs to be sent and received with guaranteed delivery regardless of the interface mode (e.g., API or batch).	M	Yes	Standard	Data entry and exchange edits are used to meet the expected data integrity error rate.
B12.6	Vendor shall replace key personnel within fifteen (15) State workdays. The State may grant additional time to replace key personnel if the Vendor makes interim arrangements to ensure that operations are not affected by loss of personnel.	M	Yes	Standard	In the event of key personnel loss, FDGS will work to replace them within 15 State workdays and will communicate our contingency plans to coordinate so as not to affect operations. Our operations team consists of multiple AuthenticCare technicians to limit risk to continued operations.
B12.7	Request and receive written approval by the Department prior to releasing any public announcement concerning the Contract, including, but not limited to, notices, information pamphlets, press releases, research, reports, signs, and similar public notices prepared by or for Vendor.	M	Yes	Standard	FDGS will coordinate with the Department on any public communication relating to this contract.
B12.8	All standardized reports shall be available online or delivered to authorized users by the scheduled time one hundred percent (100%) of the time as defined and mutually agreed upon during detailed report design. Penalties will not be assessed during system downtime due to scheduled maintenance.	M	Yes	Standard	AuthenticCare reports are available through our online web site to protect PII/PHI data. Reports are available on demand or through our scheduler. They will be available 100% of the time as defined and mutually agreed.
B12.9	Vendor must notify the State of any data load problems, discrepancies, or failures within one (1) workday of identification and present a resolution plan within three (3) workdays.	M	Yes	Standard	FDGS Operations uses monitoring and review of data load processes to identify issues. We will notify the State within 1 business day and, as needed, present a resolution plan within 3 business days.
B12.10	Vendor must have the capability to exchange and interface data with systems of record and process updates in near real time (within 3 seconds 99% of the time) transactions, excluding batch interface updates. Performance is measured by a predefined sample measuring the timestamp data was received to the timestamp the data is available to query in the database or presented to the user via a user interface.	M	Yes	Standard	AuthenticCare supports both real-time and batch interfaces. For real-time interfaces data will be available for review and reporting within 3 seconds 99% of the time. Updates are made to our transactional database tables where data is retrieved for viewing. Reporting typically is drawn from our Disaster Recovery database and is available in this same time requirement.
B12.11	Vendor must receive data from third party / provider EVV systems and system of records (state systems) in near real time (within 3 seconds 99% of the time), excluding batch interface updates. Performance is measured by a predefined sample measuring the timestamp data was received to the timestamp the data is available to query in the database or presented to the user via a user interface.	M	Yes	Standard	AuthenticCare Aggregator accepts visit data in near real time from third-party / provider EVV systems and state systems through our web services as well as via batch if least burdensome for the provider.
B12.12	Vendor must demonstrate requirement compliance for one hundred percent (100%) of the requirements defined for each Department requested system modification by providing documentation such as system, integration, or parallel test results or demonstration of the specifications including interfaces/APIs when requested. Compliance must be met by the Department approved implementation date.	M	Yes	Standard	FDGS will provide the required documentation to demonstrate requirement compliance for Department requested mutually agreed upon modifications to our EVV solution.
B12.13	The Vendor's help desk shall answer all calls within two (2) minutes or less of entering the queue, as determined based on the monthly average. The call abandonment rate shall be less than five percent (5%) as measured on a monthly basis.	M	Yes	Standard	FDGS agrees to these service levels for call answer time and abandonment rate.
B12.14	Vendor must respond to written, faxed, or emailed inquiries within two (2) business days of receipt.	M	Yes	Standard	FDGS will respond to inquiries within two business days of our receipt.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

B12.15	The Vendor shall ensure all customer service interactions are logged in the Vendor's information systems with ninety-five percent (95%) of all issues resolved on the same day and one hundred percent (100%) of issues resolved within 30 days.	M	Yes	Standard	FDGS shares the expectation for prompt resolution for all customer service interactions with our AuthenticCare help desk. We currently track toward this service level and agree to resolve 95% of all logged customer service interactions within 1 business day. Enhanced focus and priority are always on the occurrence of any Class A deficiency/defect. However, most if not all customer service interactions are resolved well before 30 days. For any more complex issues that would go past the 30 day limit, we provide regular communication on actions and progress toward resolution.
B12.16	Class A Deficiencies/Defects - The Vendor shall have available to the State on-call telephone assistance, with issue tracking available to the State, eight (8) hours per day and five (5) days a week with an email / telephone response within two (2) hours of request; Class B & C Deficiencies/Defects -The State shall notify the Vendor of such Deficiencies/Defects during regular business hours and the Vendor shall respond back within four (4) hours of notification.	M	Yes	Standard	The AuthenticCare Tier 1 Call Center is accessible through email and telephone 8:00 a.m. to 8:00 p.m. Monday through Friday, Eastern Time, excluding holidays. Agents create incident tickets in our Servicetow system for tracking purposes. FDGS will respond within 2 hours for Class A issues and 4 hours for Class B & C during these hours.
B12.17	Provide the Vendors plan for resolution within two (2) hours of the notification of the Class A deficiency to the Department and resolve the deficiency within twenty-four (24) hours of the notification of the deficiency to the Department.	M	Yes	Standard	For deficiencies agreed to be Class A, FDGS will provide a resolution plan within 2 hours of identification with a target to resolve within 24 hours. FDGS technicians are available 24x7 for Class A issues.
B12.18	Provide the Vendors plan for resolution within four (4) hours of the notification of the Class B deficiency/defect to the Department and resolve the deficiency within thirty-six (36) hours of the notification of the deficiency to the Department.	M	Yes	Standard	For deficiencies agreed to be Class B, FDGS will provide a resolution plan within 4 hours of identification with a target to resolve within 36 hours.
B12.19	Produce and distribute new publications or amended publications in final form by the date requested by the Department.	M	Yes	Standard	FDGS will produce and distribute new or amended publications for the AuthenticCare EVV solution in final form by a mutually agreed upon date.
B12.20	Maintain up to date functional documentation, including both user documentation and the Operations Procedure Manual.	M	Yes	Standard	FDGS maintains up to date documentation for AuthenticCare including user manual, reference guides and release notes of changes.
B12.21	Training documentation shall be updated no more than ten (10) Business Days after the implementation of a software change.	M	Yes	Standard	AuthenticCare training documentation is updated as system modifications require. It will be updated in no more than 10 business days after a change is implemented.
B12.22	Vendor shall make available all required reports in accordance with stated timeliness requirements.	M	Yes	Standard	AuthenticCare reports are available through our online web site to protect PII/PHI data. Reports are available on demand or through our scheduler. They will be available 100% of the time as defined and mutually agreed.
B12.23	The Vendor shall attend all meetings as required by the Department if advance notice is provided. The Department will stipulate whether in-person or remote/virtual attendance is required. Advance notice is defined as at least three (3) Business Days prior to the meeting start time.	M	Yes	Standard	FDGS agrees to attend all Department required meetings given advance notice.
B12.24	System change orders/requests shall be implemented by the mutually agreed upon due date.	M	Yes	Standard	Change orders relating to the FDGS contract will be implemented by the mutually agreed upon date as documented in our Statement of Work (SOW).

Exhibit G, Attachment 1
EVV Business and Technical Requirements

B12.25	Restore availability within twenty-four (24) hours from the start of any disaster event involving the Vendor's solution, using procedures approved in the Business Continuity and Contingency Plan and the Disaster Recovery Plan.	M	Yes	Standard	<p>FDGS has documented Business Continuity and Disaster Recovery Plans. These are tested annually with Disaster Recovery processing live activity for several days to a week at our secondary data center. Our most recent test showed a restoration in less than 4 hours. Data is replicated in real time between our geographically diverse data centers in Chandler AZ and Omaha NE. Each data center has full staffing and redundant environmental and power systems in addition to duplicate servers for full capacity. Within each data center multiple servers are load balanced to limit the impact created by a failure in any one server or piece of hardware.</p> <p>Our Business Continuity Plan specifies critical business functions and systems and documents the plan should those become unavailable. The biggest test of BCP has been the COVID pandemic where FDGS staff were immediately able to work from home when leadership deemed it not safe to work in the office.</p> <p>Recovery Time Objective and Recovery Point Objective are documented. Database backups are taken and distributed across our data centers so they do not leave our facilities but are stored across geography. Full backups are taken nightly with iterative backups completed throughout the day. This coupled with the database replication minimizes the risk of data loss.</p>
B12.26	The Vendor will be held accountable for and must reimburse the Department for any EVV related claims paid as a result of any error on the Vendor's part, which exceed or do not comport with the service limitations or prior authorized amount, including any penalties that are assessed by a Federal agency due to this error.	M	Yes	Standard	<p>FDGS puts in place the business rules, data integrity edits and operational controls to prevent processing errors from occurring. However, we understand that any potential error on our part may result in unauthorized payments. FDGS will work with the Department to resolve/recover as much of the amount paid in error to minimize any liability.</p>

Exhibit G, Attachment 1
EVV Business and Technical Requirements

APPLICATION REQUIREMENTS					
State Requirements			Vendor		
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
GENERAL SPECIFICATIONS					
A1.1	Ability to access data using open standards access protocol (please specify supported versions in the comments field).	M	Yes	Standard	AuthentiCare supports data access using open standards including XML, EDI X12 version 5010 and CSV and Excel current version -1.
A1.2	Data is available in commonly used format over which no entity has exclusive control, with the exception of National or International standards. Data is not subject to any copyright, patent, trademark or other trade secret regulation.	M	Yes	Standard	EVV and associated data collected in AuthentiCare is owned by the State. It is not subject to any legal regulation. Data is available in commonly used formats such as XML and CSV as well as HIPAA X12 EDI for State or stakeholder use.
A1.3	Web-based compatible and in conformance with the following W3C standards: HTML5, CSS 2.1, XML 1.1	M	Yes	Standard	AuthentiCare is a web based application compatible and in conformance with HTML5, CSS 2.1, and XML 1.1.
APPLICATION SECURITY					
A2.1	Verify the identity or authenticate all of the system client applications before allowing use of the system to prevent access to inappropriate or confidential data or services.	M	Yes	Standard	For all web and web service connections to the AuthentiCare platform, including mobile transactions, FDGS requires TLS 1.2 Transport Level Security. The mobile apps employ certificate pinning for resistance to "man in the middle" attack. File transfers use the First Data File Gateway hosted SFTP site, and are AES 256-bit encrypted according to FIPS 140-2 requirements. From an authentication and access standpoint, AuthentiCare supports Multi-Factor Authentication (MFA) with a username/password combination as "something you know" and device id or QR code for mobile and One Time Pin (OTP) emailed from our pingfederate system for web as "something you have".
A2.2	Verify the identity and authenticate all of the system's human users before allowing them to use its capabilities to prevent access to inappropriate or confidential data or services.	M	Yes	Standard	FDGS works with DHHS during the implementation process to identify an initial set of users for whom to create accounts. Those users then have the ability to create accounts for additional users within their organizations. All AuthentiCare access is authorized through our login process. Only a few specific users are granted the administrative role allowing the designation for other user access. AuthentiCare supports Multi-Factor Authentication (MFA) with a username/password combination as "something you know" and device id or QR code for mobile and One Time Pin (OTP) emailed from our pingfederate system for web as "something you have".
A2.3	Enforce unique user names.	M	Yes	Standard	AuthentiCare enforces the use of unique usernames. A unique email account must be on file for AuthentiCare web access as part of the multi-factor authentication process.
A2.4	Enforce complex passwords for Administrator Accounts in accordance with DoIT's statewide User Account and Password Policy.	M	Yes	Standard	FDGS follows NIST 800-63B Digital Identity Guidelines. AuthentiCare supports state-specific configuration for password length, complexity, history policy, dictionary checks and expiration timeframe as long as state password policies meet minimum requirements enforced by our corporate policy. AuthentiCare allows states to apply stricter rules if desired.
A2.5	Enforce the use of complex passwords for general users using capital letters, numbers and special characters in accordance with DoIT's statewide User Account and Password Policy.	M	Yes	Standard	AuthentiCare supports state-specific configuration for password length, complexity, history policy, dictionary checks and expiration timeframe as long as state password policies meet minimum requirements enforced by our corporate policy. AuthentiCare allows states to apply stricter rules if desired.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

A2.6	Encrypt passwords in transmission and at rest within the database.	M	Yes	Standard	<p>Passwords are encrypted during transmission through HTTPS TLS 1.2 SSL certificates.</p> <p>At rest, password are stored using a one-way hash with SALT and cannot be recovered if forgotten. Mobile app password are stored in the AuthenticCare portal and compared as an SHA 512-bit encrypted hash, so that only the mobile user knows the pass phrase used to generate the hash. Our self-service password reset function is used to reset unknown password.</p>
A2.7	Establish ability to expire passwords after a definite period of time in accordance with Dolt's statewide User Account and Password Policy.	M	Yes	Standard	<p>Password expiration after a number of days is configurable to align with Dolt's statewide policy. FDGS policy is used as a minimum requirement.</p>
A2.8	Provide the ability to limit the number of people that can grant or change authorizations.	M	Yes	Standard	<p>Access to manage authorizations is limited to those who have been assigned to the roles with the associated rights to create and edit authorizations.</p>
A2.9	Establish ability to enforce session timeouts during periods of inactivity.	M	Yes	Standard	<p>Session timeouts are configurable and must, at a minimum, comply with FDGS policy.</p>
A2.10	The application shall not store authentication credentials or sensitive data in its code.	M	Yes	Standard	<p>AuthenticCare does not store authentication credentials or sensitive data in its code.</p>
A2.11	Log all attempted accesses that fail identification, authentication and authorization requirements.	M	Yes	Standard	<p>AuthenticCare maintains an audit trail of all successful and unsuccessful logins including the date, time and type of failure.</p>
A2.12	The application shall log all activities to a central server to prevent parties to application transactions from denying that they have taken place.	M	Yes	Standard	<p>AuthenticCare uses centralized logging that includes detailed interactions with mobile devices, IVR activity and access through the website and data interfaces.</p>
A2.13	All logs must be kept for 90 days.	M	Yes	Standard	<p>Detailed AuthenticCare logs are stored for 90 days. Audit trails for login, access, and changes to data are maintained per agreed upon data retention plans.</p>
A2.14	The application must allow a human user to explicitly terminate a session. No remnants of the prior session should then remain.	M	Yes	Standard	<p>When a user logs out of AuthenticCare, their session is terminated and data does not remain on their computer.</p>
A2.15	Do not use Software and System Services for anything other than they are designed for.	M	Yes	Standard	<p>Software and system services are only used for their intended purpose. Support personnel are assigned unique, individual accounts for their use and are not permitted to use system accounts for support purposes.</p>
A2.16	The application Data shall be protected from unauthorized use when at rest.	M	Yes	Standard	<p>Access to application data at rest is limited to our support organization. FDGS provides column-level encryption of PII and PHI data at rest using Voltage encryption tools to prevent direct access.</p>

Exhibit G, Attachment 1
EVV Business and Technical Requirements

A2.17	The application shall keep any sensitive Data or communications private from unauthorized individuals and programs.	M	Yes	Standard	<p>Data is protected using encryption at rest and in transit and multi-factor authentication is used to authorize access. To further protect PII/PHI, AuthenticCare encrypts the data at the column level and in files at rest using Micro Focus' Voltage. This is an API-based process making the data only available through authorized access into logged application interfaces. PII/PHI cannot be read directly in the database or on disk storage. In addition to monitoring network connections and incoming traffic, Fiserv maintains and monitors a Data Loss Prevention (DLP) system to prevent egress of network data and email traffic containing PHI/PII. This additional check on outgoing flow of specific types of data offers extra protection by preventing specific data from leaving our secure environment.</p> <p>Our Defense in Depth security model provides an extensive system of physical, technical and administrative controls to protect EVV data through system access security, network security, application design and security, physical access security, and data security and encryption. FDGS is also audited annually by several independent third-party auditors. FDGS audits are performed by these three broadly recognized assessors: SSAE-18 SOC 1 and SOC 2 (Deloitte & Touche), PCI DSS (Trustwave) and HIPAA/HITECH (Optiv). Our privacy principle respects and protects the individuals, while adhering to regulatory requirements. AuthenticCare will meet the latest compliance, privacy and security standards.</p>
A2.18	Subsequent application enhancements or upgrades shall not remove or degrade security requirements.	M	Yes	Standard	<p>Security review is built into our Software Development Life Cycle (SDLC). Every release includes security scans and our change management process does not allow software with Critical or High vulnerabilities to be promoted to production. Moderate and Low vulnerabilities are tracked and must be remediated within a policy determined timeframe (180 days for Moderate and 365 days for Low).</p>
A2.19	Utilize change management documentation and procedures.	M	Yes	Standard	<p>FDGS follows a documented change management process overseen by an independent team of change managers whose approval must be given for implementations into production. Software development follows our Software Development Life Cycle (SDLC) requiring promotion of code from Development environments to Quality Assurance to User Acceptance to Production and Disaster Recovery.</p> <p>Part of the process includes a detailed implementation plan explaining what each team's tasks are for an implementation. This includes backout planning should there be an issue during the implementation.</p> <p>These processes are reviewed by our third party audit as part of our SOC 2.</p>
A2.20	Web Services : The service provider shall use Web services exclusively to interface with the State's data in real time/near real time when possible.	M	Yes	Standard	<p>Web services are the preferred interface for FDGS where possible as well. AuthenticCare has several client who access visit data via our web services and we also have integrated with our customer's web services to retrieve data such as members, providers, authorizations and submit visits.</p>

Exhibit G, Attachment 1
EVV Business and Technical Requirements

TESTING REQUIREMENTS					
State Requirements			Vendor		
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
APPLICATION SECURITY TESTING					
T1.1	All components of the Software shall be reviewed and tested to ensure they protect the State's web site and its related Data assets.	M	Yes	Standard	AuthentiCare application goes through the Application Certification and Authorization (ACA) process for approval to operate, and to resolve hardware, infrastructure, and software security findings. Each release is subject to peer review and multiple scan engines including Fortify, WebInspect and Sonatype. Critical and High vulnerabilities must be remediated prior to production installation as controlled by our independent change managers. Moderate and Low findings are also addressed by today's policy of 180 days and 365 days respectively.
T1.2	The Vendor shall be responsible for providing documentation of security testing, as appropriate. Tests shall focus on the technical, administrative and physical security controls that have been designed into the System architecture in order to provide the necessary confidentiality, integrity and availability.	M	Yes	Standard	FDGS completes independent third-party audits that confirm we meet the controls for confidentiality, integrity and availability such as SOC 2, HIPAA and PCI-DSS audits as well as our Application Certification and Authorization (ACA).
T1.3	Provide evidence that supports the fact that Identification and Authentication testing has been recently accomplished; supports obtaining information about those parties attempting to log onto a system or application for security purposes and the validation of users.	M	Yes	Standard	FDGS completes independent third party audits that confirm we meet the controls for confidentiality, integrity and availability such as SOC 2, HIPAA and PCI-DSS audits as well as our Application Certification and Authorization (ACA). These audits require evidence and interviews to verify identification, authorization and auditing testing is in place.
T1.4	Test for Access Control; supports the management of permissions for logging onto a computer or network.	M	Yes	Standard	FDGS completes independent third-party audits that confirm we meet the controls for confidentiality, integrity, and availability such as SOC 2, HIPAA and PCI-DSS audits as well as our Application Certification and Authorization (ACA). These audits require evidence and interviews to verify the access controls are in place.
T1.5	Test for encryption; supports the encoding of data for security purposes, and for the ability to access the data in a decrypted format from required tools.	M	Yes	Standard	AuthentiCare uses AES 256-bit encryption for data at rest along with Transport Level Security (TLS) 1.2 for data in transit. Web and mobile passwords are stored as an SHA 512 one-way hash meaning they cannot be decrypted. AuthentiCare data scoping uses established relationships between providers, workers, recipients and their agencies to control access to user data. In addition, column level encryption is in place within the AuthentiCare databases and files at rest to protect Personal Health Information (PHI) using Microfocus' Voltage.
T1.6	Test the Intrusion Detection; supports the detection of illegal entrance into a computer system.	M	Yes	Standard	Internet connectivity to the network is protected by a firewall complex that uses leading commercial firewalls and various Intrusion Detection/Protection techniques. Intrusion Detection is in place on the following segments: Internet point-of-presence, DMZ, Extranet, internal production network and network segment hosting target data. It is configured to generate alerts in case of incidents and values exceeding the environment's normal thresholds. We have a formal process to regularly update the IDS signatures based on new threats and changes in the environment.
T1.7	Test the Verification feature; supports the confirmation of authority to enter a computer system, application or network.	M	Yes	Standard	Application access requires multi-factor authentication and is role-based restricting access to a need-to-know policy. Penetration testing performed by our Internal and third-party assessors verifies these security features during standard cycles.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

T1.8	Test the User Management feature; supports the administration of computer, application and network accounts within an organization.	M	Yes	Standard	Our Security Administrators responsible for managing user account provisioning develop and manage procedures for the process of user provisioning for business-to-consumer as well as business-to-business access of FDGS data. These procedures detail the following major tasks: Enrollment: This process must be incorporated within application design. Approval: Approval of such access must follow defined procedures for FDGS role-based access, which is built upon least privilege and need-to-know.
T1.9	Test Role/Privilege Management; supports the granting of abilities to users or groups of users of a computer, application or network.	M	Yes	Standard	Our Security Administrators responsible for managing user account provisioning develop and manage procedures for the process of user provisioning for business-to-consumer as well as business-to-business access of FDGS data. These procedures detail the following major tasks: Enrollment: This process must be incorporated within application design. Approval: Approval of such access must follow defined procedures for FDGS role-based access, which is built upon least privilege and need-to-know.
T1.10	Test Audit Trail Capture and Analysis; supports the identification and monitoring of activities within an application or system.	M	Yes	Standard	During the testing phase FDGS validates that the following are maintained: audit trail of changes to data, such as visits and authorizations; user access, like login, logout and account locks; and HIPAA logging for what user accessed PHI/PHI data.
T1.11	Test Input Validation; ensures the application is protected from buffer overflow, cross-site scripting, SQL injection, and unauthorized access of files and/or directories on the server.	M	Yes	Standard	FDGS applications are scanned as part of our SDLC. In addition to peer reviews, tools including Fortify, WebInspect and Sonatype are used that include the OWASP Top Ten. These occur at a minimum of every 90 days or more frequently while under active development. Manual and other automated tools are used by our independent Application Security Assessment (ASA) team. In addition, AuthenticCare has been and will continue to be reviewed by independent third parties as part of ongoing CMS certification activity with our customers. Applications are designed to prevent buffer overflows— unintended overwriting of data and program memory space. As such, data input into application systems are validated by performing checks.
T1.12	For web applications, ensure the application has been tested and hardened to prevent critical application security flaws. (At a minimum, the application shall be tested against all flaws outlined in the Open Web Application Security Project (OWASP) Top Ten (http://www.owasp.org/index.php/OWASP_Top_Ten_Project).	M	Yes	Standard	FDGS applications are scanned as part of our SDLC. In addition to peer reviews, tools including Fortify, WebInspect and Sonatype are used that include the OWASP Top Ten. These occur at a minimum of every 90 days or more frequently while under active development. Manual and other automated tools are used by our independent Application Security Assessment (ASA) team. In addition, AuthenticCare has been and will continue to be reviewed by independent third parties as part of ongoing CMS certification activity with our customers.
T1.13	Provide the State with validation of 3rd party security reviews performed on the application and system environment. The review may include a combination of vulnerability scanning, penetration testing, static analysis of the source code, and expert code review (please specify proposed methodology in the comments field).	M	Yes	Standard	FDGS completes independent third-party audits that confirm we meet the controls for confidentiality, integrity and availability such as SOC 2, CMS, HIPAA and PCI-DSS audits as well as our Application Certification and Authorization (ACA). FDGS will provide validation of our security reviews.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

T1.14	Prior to the System being moved into production, the Vendor shall provide results of all security testing to the Department of Information Technology for review and acceptance.	M	Yes	Standard	Development and maintenance activity to the production IT environment, including changes to application systems, supporting system software, hardware, security infrastructure and telecommunication systems, is performed in accordance with a standard Software Development Life Cycle (SDLC). The SDLC is a complete business process and systems engineering methodology which requires development and testing, including security testing, prior to production deployment. Additionally, our change management process requires business owner to submit testing and security results to the change board prior to production implementation. Results of security testing will be provided to DoIT prior to initial production deployment of the system.
T1.15	Vendor shall provide documented procedure for migrating application modifications from the User Acceptance Test Environment to the Production Environment.	M	Yes	Standard	The SDLC is a complete business process and systems engineering methodology. The SDLC requires testing and sign-off for promoting application modifications from Dev to QA environment, from QA to UAT environments and from UAT to Production. Change management process requires business owner to submit the testing and security to the change board prior to production implementation.
STANDARD TESTING					
T2.1	The Vendor must test the software and the system using an industry standard and State approved testing methodology.	M	Yes	Standard	FDGS uses industry best practices to develop the entrance and exit criteria for each project phase, requiring customer approval before initiation of subsequent phases in a waterfall or hybrid project. These criteria control entrance and exit to the Configuration Testing, Deployment, and Operations and Maintenance phases. FDGS will work with the State to establish specific criteria for progression through phases and these must be approved by the State prior to proceeding beyond the Planning and Administration tasks. The testing approach, objectives, schedule and procedures are documented in our Master Test Plan (MTP) along with phase entrance and exit criteria. Entrance criteria are documented with the primary responsibility for each item. Testing consists of promoting the configured system through our dedicated QA and UAT environments. Our teams provide iterative system testing through our Quality Management and Testing approach as well as User Acceptance Testing by the AuthenticCare team and DHHS. FDGS follows a disciplined Quality Assurance (QA) approach that contributes to our record of delivering projects on time, within budget, and with high quality. This Structured Test Methodology (STM) verifies that all functional and system-wide requirements are complete and confirms the configuration requirements.
T2.2	The Vendor must perform application stress testing and tuning.	M	Yes	Standard	All application releases are subject to stress/load testing activities that simulate heavy production cycles to confirm that code modifications are production ready.
T2.3	The Vendor must provide documented procedure for how to sync Production with a specific testing environment.	M	Yes	Standard	FDGS will provide our documented procedures for keeping Production and Testing environments in sync. FDGS maintains multiple testing environments as part of our Software Development Life Cycle (SDLC). Software and configuration changes are promoted from lower level environments (Development, Quality Assurance (QA), User Acceptance Testing (UAT), and Production/Disaster Recovery). Changes are evaluated in each promotion step to confirm expected results. FDGS supports a rigorous change management process that is reviewed annually by our third party auditors. One of our User Acceptance Testing environments runs the current production release of AuthenticCare. This is used for testing and troubleshooting issues reported in production. A second UAT environment is our production path. It runs the next release of AuthenticCare as it is being validated prior to being implemented for production use.

RFP-2022-DLTSS-05-ELECT-01 #2022-031

First Data Government Solutions, Limited Partnership

Exhibit G, Attachment 1, EVV Business and Technical Requirements

Contractor Initials: SM
Date: 9/2/2022

Page 31

Exhibit G, Attachment 1
EVV Business and Technical Requirements

12.4	The vendor must define and test disaster recovery procedures.	M	Yes	Standard	FDGS has a documented disaster recovery (DR) plan for AuthenticaCare that is exercised annually. During this test, and in coordination with our customers, live production activity is processed at our DR facility in Omaha, NE for several days. Results of the test are documented for process improvement identification. After the test has been completed, live activity is moved back to the primary data center in Chandler, AZ. Customers are invited to participate in the DR exercise.
------	---	---	-----	----------	---

Exhibit G, Attachment 1
EVV Business and Technical Requirements

HOSTING-CLOUD REQUIREMENTS					
State Requirements			Vendor		
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
OPERATIONS					
H1.1	Vendor shall provide an ANSI/TIA-942 Tier 3 Data Center or equivalent. A tier 3 data center requires: 1) Multiple independent distribution paths serving the IT equipment, 2) All IT equipment must be dual-powered and fully compatible with the topology of a site's architecture, and 3) Concurrently maintainable site infrastructure with expected availability of 99.982%.	M	Yes	Standard	Our Chandler and Omaha Data Centers are built to ANSI/TIA-942 standards. 1. Three independent power systems deliver UPS back power to the Data Center space. All hardware is connected to two of these for redundancy. Any two of the three services has the capacity to support data center loads at the 4.8MW capacity. 2. All network and computer hardware is required to have dual power supplies configured such that either one of the two can support the operation of the equipment 3. Not more than one of the three power sources is in a maintenance mode at any time. Maintenance may be performed without interruption to the service being worked on.
H1.2	Vendor shall maintain a secure hosting environment providing all necessary hardware, software, and Internet bandwidth to manage the application and support users with permission based logins.	M	Yes	Standard	AuthentiCare is hosted in our geographically diverse data centers located in Chandler, AZ and Omaha, NE. Our SaaS offering includes all hardware, software, network access and internet bandwidth required to host your AuthentiCare solution. On an ongoing basis, our policies are reviewed and approved by these three broadly recognized assessors—SOC 1/SOC 2/SSAE-18 (Ernst & Young/Deloitte), PCI DSS (Trustwave) and GLBA (Federal Financial Institutions Examination Council [FFIEC])—as well as many state, local and customer assessors. FDGS has established a Global Cyber Security Policy in alignment with the NIST CSF (National Institute of Standards and Technology, Cyber Security Framework), which is based on a subset of controls within the comprehensive NIST SP 800-53 r4 controls. The Global Cyber Security Policy is fully complementary to the ISO (International Standards organization) 27001-2013 cyber security controls, with certain geographic areas maintaining ISO 27001-2013 certification. FDGS can provide a copy of our annual SOC 2 Report as a separate file upon request.
H1.3	The Data Center must be physically secured – restricted access to the site to personnel with controls such as biometric, badge, and others security solutions. Policies for granting access must be in place and followed. Access shall only be granted to those with a need to perform tasks in the Data Center.	M	Yes	Standard	Badge access systems are installed at all FDGS facilities to restrict access along with manual controls, biometric electronic locks and PIN-restricted turnstiles. Card keys contain a photo ID of the employee and must be worn at all times. Data Centers are protected with wrought iron pillars and multiple layers of fence. Access is only granted to those who need to perform specific tasks in the Data Center and multiple levels of approval are required.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

H1.4	Vendor shall install and update all server patches, updates, and other utilities within 60 days of release from the manufacturer.	M	Yes	Standard	<p>System maintenance occurs at least monthly and systems are patched in accordance with our Cyber Security standard. Monthly patching occurs based on schedules defined within the FDGS patching portal, with ad hoc patching available if Cyber Team deems a patch to be critical. Once a patch is approved for deployment, FDGS has a dedicated patch team that applies updates and patches.</p> <p>FDGS monitors our hardware vendors for updates related to physical hardware vulnerabilities. Switches, disk arrays, BIOS and other devices are remediated with priority based on our Cyber Threat Intelligence team's and Security Operations Center's risk assessment of the reported threat. All patching, regardless of criticality, follows our Global Change Management policies and procedures. FDGS adheres to the NIST standards on the vulnerability impacts and criticality of risk. FDGS patch management protocol calls for rigorous pre-deployment testing. Maintenance items are tested in the engineering lab and are promoted and validated in lower environments prior to production deployment.</p>
H1.5	Vendor shall monitor System, security, and application logs.	M	Yes	Standard	<p>Immutable operational logs are stored both at the system and application levels. Logs are maintained in compliance with our security policies including retention periods. Infrastructure logs are held at the system level and forwarded to our centralized logging environment for monitoring and review. Application logs are database stored with read-only availability to our support technicians for troubleshooting purposes.</p> <p>To support regulatory compliance, including HIPAA, all systems associated with processing, storing or transmitting PHI or PII must generate log files of all activity. These activities are itemized in the Cyber Security Logging Standard. Authenticare operational log files provide data to support our cyber security logging and monitoring functions. Included in this logging activity is an audit trail of changes to the EVV data. Logging is also in place for user access to the data should questions of appropriateness require review.</p> <p>FDGS is compliant with NIST standards including privacy, security, authorization control and continuous monitoring. This includes equivalent security to that of the Federal Risk and Authorization Management Program (FedRAMP), a U.S. government program that delivers a standard approach to the security assessment, authorization and continuous monitoring specifically for federal agency cloud deployments and services.</p>
H1.6	Vendor shall manage the sharing of data resources.	M	Yes	Standard	<p>FDGS manages the sharing of data resources both from a physical and logical standpoint. Controls are in place in our virtual environment to allocate resources to our servers when needed. This includes CPU, Memory and Storage. In terms of logical sharing, Authenticare is designed to provide access to any authorized users at the time data is requested only locking data when required for updates.</p>

Exhibit G, Attachment 1
EVV Business and Technical Requirements

H1.7	Vendor shall manage daily backups, off-site data storage, and restore operations.	M	Yes	Standard	<p>AuthentiCare data are stored in a database cluster with nodes in both our Chandler and Omaha data centers providing a current copy of data for Disaster Recovery purposes. Full backups are taken daily, when user activity is low. In addition, transaction logs are backed up at five minutes to the hour every day. In the event of a database failure, this combination of backups—transaction log and full database—provides the requisite input source to recover the database up to the time that the failure occurred (point in time recovery). As part of our standard disaster recovery and business continuity plans, the AuthentiCare recovery and restore plans are tested annually.</p> <p>Data backups collected from the AuthentiCare system are securely stored at geographically dispersed network data backup locations spread across Fiserv facilities as an extra safety measure. The backups are encrypted and networked across a distributed storage infrastructure so that the data never leaves a secure Fiserv facility and captive network but maintains redundancy across facilities so data are protected from loss at any one facility. This eliminates the need for off-site storage using magnetic media that would require secure handling, storage and sanitation according to NIST SP 800-88.</p>
H1.8	The Vendor shall monitor physical hardware.	M	Yes	Standard	<p>FDGS uses AppDynamics Performance Monitor (APM), a suite of tools to maintain stability and availability of the AuthentiCare solution platform. APM also allows FDGS to monitor the performance of the key business functions of AuthentiCare within the hardware and software infrastructure layers.</p> <p>Based on monitoring results, it creates alerts on critical resources component utilization or when response thresholds are exceeded so that proper action can take place to restore normal functioning and performance of the systems. We have real-time data capture and archives used for performance and utilization trending that drives our capacity review and upgrade processes.</p> <p>The FDGS data center operations team maintains dashboards, performance statistics and alerts in the AppDynamics tool to monitor business activity by business process in real time.</p>
H1.9	Remote access shall be customized to the State's business application. In instances where the State requires access to the application or server resources not in the DMZ, the Vendor shall provide remote desktop connection to the server through secure protocols such as a Virtual Private Network (VPN).	M	Yes	Standard	<p>Access required by our customers in support of AuthentiCare activities is available through the secure AuthentiCare website using TLS 1.2 SSL certificates and multi factor authentication.</p> <p>As a SaaS solution, the FDGS team of experts will address any application or server related issues including repair or replacement hardware or software and associated diagnostics and troubleshooting.</p>
H1.10	RESERVED				Not Applicable
DISASTER RECOVERY					

Exhibit G, Attachment 1
EVV Business and Technical Requirements

H2.1	Vendor shall have documented disaster recovery plans that address the recovery of lost State data as well as their own. Systems shall be architected to meet the defined recovery needs.	M	Yes	Standard	<p>Our hosted AuthenticCare EVV solution provides a robust, enterprise-level approach to backup and recovery to maintain business continuity. We integrate a comprehensive backup and recovery approach within our extensive Disaster Recovery and Business Continuity plans to give the State confidence that the EVV system is up and running through unexpected events or threats.</p> <p>Our approach to disaster recovery focuses on restoring the firm's critical systems and applications used by our internal businesses and external clients. Application recovery is prioritized based on the Recovery Time Objective identified in the Business Impact Analysis. FDGS maintains Disaster Recovery Procedures for key systems and applications, which provide detailed plans for restoration of service. These procedures address key personnel, components and applications that are necessary to minimize the impact to vital business processes. Our DR plan is tested annually with production activity processing in our backup site for multiple days before reverting back to our primary data center.</p>
H2.2	The disaster recovery plan shall identify appropriate methods for procuring additional hardware in the event of a component failure. In most instances, systems shall offer a level of redundancy so the loss of a drive or power supply will not be sufficient to terminate services; however, these failed components will have to be replaced.	M	Yes	Standard	<p>FDGS has service contracts on our hardware with vendors who are responsible for replacing any failed components. The systems are deployed in a highly redundant fashion in VMWare clusters that provide redundancy at the hardware level. OS images can run on any machine in the cluster and if there is a failure then the workload is automatically moved to another host while the one that has an issue is serviced.</p> <p>All the hosts deployed have multiple redundant power supplies and SAN Disk that run in RAID arrays to protect against failures. There are multiple spare disks in a array and if there is a failure then the failed disk information is rebuilt onto one of the spares. The vendor then is dispatched to replace the failed disk.</p>
H2.3	Vendor shall adhere to a defined and documented back-up schedule and procedure.	M	Yes	Standard	<p>AuthenticCare data are stored in a database cluster with nodes in both our Chandler and Omaha data centers providing a current copy of data for Disaster Recovery purposes. Full backups are taken daily, when user activity is low. In addition, transaction logs are backed up at five minutes to the hour every day. In the event of a database failure, this combination of backups—transaction log and full database—provides the requisite input source to recover the database up to the time that the failure occurred (point in time recovery). As part of our standard disaster recovery and business continuity plans, the AuthenticCare recovery and restore plans are tested annually.</p> <p>Data backups collected from the AuthenticCare system are securely stored at geographically dispersed networked data backup locations spread across Fiserv facilities as an extra safety measure. The backups are encrypted and networked across a distributed storage infrastructure so that the data never leaves a secure Fiserv facility and captive network but maintains redundancy across facilities so data are protected from loss at any one facility. This eliminates the need for off-site storage using magnetic media that would require secure handling, storage and sanitation according to NIST SP 800-88.</p>
H2.4	Back-up copies of data are made for the purpose of facilitating a restore of the data in the event of data loss or System failure.	M	Yes	Standard	SQL replication and bandwidth between the data centers enables near real-time data continuity and replication allowing for minimized recovery point objectives (RPOs).
H2.5	Scheduled backups of all servers must be completed regularly. The minimum acceptable frequency is differential backup daily, and complete backup weekly.	M	Yes	Standard	Full backups are taken daily, when user activity is low. Additionally, transaction logs are backed up at five minutes to the hour every day. In the event of a database failure, this combination of backups—transaction log and full database—provides the requisite input source to recover the database up to the time that the failure occurred (point in time recovery). As part of our standard disaster recovery and business continuity plans, the AuthenticCare recovery and restore plans are tested annually.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

H2.6	Tapes or other back-up media tapes must be securely transferred from the site to another secure location to avoid complete data loss with the loss of a facility.	M	Yes	Standard	FDGS backups maintained across multiple US data centers means that physical tape media is not used so there is no need for chain of possession security nor risk of loss of tapes. Your data remains within our own US-based data centers protected from loss of facility as described above. Therefore, this requirement is not applicable.
H2.7	Data recovery – In the event that recovery back to the last backup is not sufficient to recover State Data, the Vendor shall employ the use of database logs in addition to backup media in the restoration of the database(s) to afford a much closer to real-time recovery. To do this, logs must be moved off the volume containing the database with a frequency to match the business needs.	M	Yes	Standard	Full backups are taken daily, when user activity is low. In addition, transaction logs are backed up at five minutes to the hour every day. In the event of a database failure, this combination of backups—transaction log and full database—provides the requisite input source to recover the database up to the time that the failure occurred (point in time recovery). As part of our standard disaster recovery and business continuity plans, the AuthentiCare recovery and restore plans are tested annually.
H2.8	Notify the Department no later than one (1) hour following a Vendor-declared Disaster.	M	Yes	Standard	Once our Joint Security Operations Center (JSOC) declares a disaster for the Omaha or Chandler data center, the FDGS Account/Operations Manager will notify the Department within one hour.
H2.9	Upon Disaster declaration, resume full functionality and operational business functions within the specified recovery time objective (RTO).	M	Yes	Standard	Upon a disaster declaration, FDGS will transfer operations to our back-up site within the specified Recovery Time Objective (RTO).
H2.10	Achieve a Complete Recovery from a Disaster or other incident within the specified RTO of one (1) hour and recovery point objective (RPO) of four (4) hours. The RTO must include application validation and testing by the Department.	M	Yes	Standard	AuthentiCare is architected with redundancy in both of our data centers to support maximum availability. This includes from the standpoint of servers, networks, internet access, telephony, power, and environmental controls. To minimize the RPO, AuthentiCare data is maintained in databases at both our primary and disaster recovery sites. It is synchronized using Microsoft SQL Server Always On. Databases are logically separated for each AuthentiCare client and use column level encryption. The data is replicated between the two data centers continually so that each site is synchronized and ready for processing. In the event of a disruption of service to the primary site, the secondary site assumes processing of the additional workload, allowing users to continue execution of service without outages or delays. During patching or unplanned outages of our DB servers, Always On listeners seamlessly provide connections to the databases in the DR environment. This enables little to no service interruption during patching, planned or unplanned outages. Upon resumption of availability, the primary database is synchronized and, when complete, the listener returns activity to the production database.
H2.11	Plan and coordinate with the Department and NH service providers to perform annual Disaster Recovery (DR) exercises, to include disaster simulation and recovery tabletop demonstrations to demonstrate DR capabilities. The DR exercise must, at a minimum, test the recovered environments, accessibility, data integrity and functionality. For annual DR exercises: a. The Department must approve the scope of each DR exercise; b. A post DR exercise lessons learned meeting must be completed no later than thirty (30) Calendar Days after completion of the DR exercise; and c. In the event of a failed DR exercise, as defined in Department approved exercise scope, the Contractor must reschedule and conduct another DR exercise no later than ninety (90) Calendar Days after the failed exercise.	M	Yes	Standard	AuthentiCare Disaster Recovery is tested annually as part of a firm-wide exercise and has demonstrated successful recovery in all recent exercises. In summer of 2021, production activity was successfully moved from Chandler to Omaha for the most recent disaster recovery test. Clients are invited to participate in all data center validation and results are distributed to clients approximately 30 days after completion of a data center exercise. The Disaster Recovery team manages and coordinates recovery activities and rigorous exercises to demonstrate the firm's ability to recover. Key systems and applications are tested regularly. Follow-up reports are generated and reviewed with all exercise participants and all issues identified are recorded in our risk management tool and tracked through resolution.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

H2.12	Coordinate with and demonstrate to the Department Business Continuity and Contingency Plan on the Department approved schedule, in conjunction with the annual DR exercise, and report any identified deficiencies with appropriate corrective actions.	M	Yes	Standard	FDGS will review our business continuity and disaster recovery approach and plans with the Department during the project planning phase. Along with the comments above for Req H2.11, please see Section IV, Topics 22, 23 and 24 for additional details surrounding our complete Business Continuity and Disaster Recovery approach.
HOSTING SECURITY					
H3.1	The Vendor shall employ security measures ensure that the State's application and data is protected.	M	Yes	Standard	FDGS is compliant with NIST standards including privacy, security, authorization control and continuous monitoring. This includes equivalent security to that of the Federal Risk and Authorization Management Program (FedRAMP), a U.S. government program that delivers a standard approach to the security assessment, authorization and continuous monitoring specifically for federal agency cloud deployments and services. FDGS is dedicated to offering a safe computing environment, safeguarding the integrity of data and maintaining proper practices to certify continued security of client data. FDGS complies with additional standards, including HIPAA (Health Insurance Portability and Accountability Act), PCI-DSS (Payment Card Industry and Data Security Standard) and CMS MITA (Medicaid Information Technology and Architecture) version 3.0. FDGS also completes an annual SOC 1 and SOC 2 (System and Organization Controls) audit with an independent third party for accreditation.
H3.2	If State data is hosted on multiple servers, data exchanges between and among servers must be encrypted.	M	Yes	Standard	TLS 1.2 encryption is in place between servers on our network.
H3.3	All servers and devices must have currently-supported and hardened operating systems, the latest anti-viral, anti-hacker, anti-spam, anti-spyware, and anti-malware utilities. The environment, as a whole, shall have aggressive intrusion-detection and firewall protection.	M	Yes	Standard	FDGS is committed to protecting the confidentiality, integrity and availability of all information within its control. To support this mission, Fiserv has established a Cyber Security Program, which protects FDGS and AuthentiCare operations in cyberspace. The program includes information security, information risk management and measures to detect and prevent fraud. We promote an environment of ethical and controlled handling of our information to verify regulatory compliance. All servers and devices have the latest anti-viral, anti-hacker, anti-spam, anti-spyware and anti-malware utilities and definitions are automatically updated. Email uses ProofPoint for anti-spam.
H3.4	All components of the infrastructure shall be reviewed and tested to ensure they protect the State's hardware, software, and its related data assets. Tests shall focus on the technical, administrative and physical security controls that have been designed into the System architecture in order to provide confidentiality, integrity and availability.	M	Yes	Standard	FDGS has established a Cyber Security Framework which is based on a subset of controls within the comprehensive NIST SP 800-53 controls that provide the confidentiality, integrity, and availability. FDGS' performs annual internal and external audits including but not limited to SOC, PCI, HIPAA and MARS-E that verifies our technical, administrative and physical controls are in place and functioning as intended.
H3.5	The Vendor shall ensure its complete cooperation with the State's Chief Information Officer in the detection of any security vulnerability of the hosting infrastructure.	M	Yes	Standard	FDGS, through our Joint Security Operations Center, coordinates with customers regarding vulnerability concerns. FDGS will work with the State's Chief Information Office and provide updates on any identified vulnerabilities to the EVV system or its data.
H3.6	The Vendor shall authorize the State to perform scheduled and random security audits, including vulnerability assessments, of the Vendor' hosting infrastructure and/or the application upon request.	M	Yes	Standard	FDGS acknowledges that the State is heavily regulated, and it has an obligation to conduct periodic due diligence of its service providers. FDGS will work with the State to determine an agreed upon process to support the State's requirement to perform security reviews. However, FDGS does not permit clients or third parties to scan or test FDGS systems or software. FDGS often facilitates reviews with clients and has prepared an Information Assurance Portfolio for clients that outlines FDGS' and its affiliates security, governance, and compliance posture.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

H3.7	All servers and devices must have event logging enabled. Logs must be protected with access limited to only authorized administrators. Logs shall include System, Application, Web and Database logs.	M	Yes	Standard	Per our Cyber Security Logging Standard, the controls below are in place for systems, applications or support processes (whether in electronic or hardcopy form): - Only system administrators have the authority to archive and delete cyber security logs - Logs must be secured to prevent alteration - Viewing must be limited to those with a job-related need - Log files must be protected from unauthorized modifications - Logs must be retained in accordance with the Record Retention Schedule
H3.8	Operating Systems (OS) and Databases (DB) shall be built and hardened in accordance with guidelines set forth by CIS, NIST or NSA.	M	Yes	Standard	FDGS' governance verifies that processes, procedures, standards and policies are used to sustain the system which conforms to industry standards and compliance guidelines. System configurations reviews are performed on a quarterly basis. Standard images are hardened to Center for Internet Security (CIS) standards and industry standards which disables unneeded services, ports and services.
H3.9	RESERVED				Not Applicable
H3.10	The Vendor shall be solely liable for costs associated with any breach of State data housed at their location(s) including but not limited to notification and any damages assessed by the courts.	M	Yes	Standard	FDGS agrees to this requirement for confirmed breaches of State data housed within our data centers.
SERVICE LEVEL AGREEMENT					
H4.1	The Vendor's System support and maintenance shall commence upon the Effective Date and extend through the end of the Contract term, and any extensions thereof.	M	Yes	Standard	FDGS will support the DHHS implementation of AuthentiCare through the end of our contract term, including extensions.
H4.2	The vendor shall maintain the hardware and Software in accordance with the specifications, terms, and requirements of the Contract, including providing, upgrades and fixes as required.	M	Yes	Standard	FDGS will maintain AuthentiCare and its supporting software and infrastructure in accordance with the agreed upon contract.
H4.3	The vendor shall repair or replace the hardware or software, or any portion thereof, so that the System operates in accordance with the Specifications, terms, and requirements of the Contract.	M	Yes	Standard	As a SaaS solution, FDGS will repair or replace hardware or software supporting the DHHS implementation of AuthentiCare per our agreed upon Contract.
H4.4	All hardware and software components of the Vendor hosting infrastructure shall be fully supported by their respective manufacturers at all times. All critical patches for operating systems, databases, web services, etc., shall be applied within sixty (60) days of release by their respective manufacturers.	M	Yes	Standard	FDGS policy requires all hardware and software components must have available vendor support. We follow a monthly patching schedule based on our monitoring of available patches from our vendors.
H4.5	The State shall have unlimited access, via phone or Email, to the Vendor technical support staff between the hours of 8:30am to 5:00pm-Monday through Friday EST.	M	Yes	Standard	FDGS Tier 1 support is available via phone or email 8:00 a.m. – 8:00 p.m. Monday through Friday Eastern Time excluding holidays. Access to these agents is not limited.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

H4.6	<p>The Vendor shall conform to the specific deficiency class as described:</p> <ul style="list-style-type: none"> o Class A Deficiency - Software - Critical, does not allow System to operate, no work around, demands immediate action; Written Documentation - missing significant portions of information or unintelligible to State; Non Software - Services were inadequate and require re-performance of the Service. o Class B Deficiency - Software - Important, does not stop operation and/or there is a work around and user can perform tasks; Written Documentation - portions of information are missing but not enough to make the document unintelligible; Non Software - Services were deficient, require reworking, but do not require re-performance of the Service. o Class C Deficiency - Software - minimal, cosmetic in nature, minimal effect on System, low priority and/or user can use System; Written Documentation - minimal changes required and of minor editing nature; Non Software - Services require only minor reworking and do not require re-performance of the Service. 	M	Yes	Standard	<p>FDGS understands the deficiency class system, as it is similar to our own. FDGS has mapped the deficiency classes to our standard incident severity levels in Section IV, Topic 14 - Testing.</p>
H4.7	<p>As part of the maintenance agreement, ongoing support issues shall be responded to according to the following:</p> <p>a. Class A Deficiencies - The Vendor shall have available to the State on-call telephone assistance, with issue tracking available to the State, eight (8) hours per day and five (5) days a week with an email / telephone response within two (2) hours of request</p> <p>b. Class B & C Deficiencies -The State shall notify the Vendor of such Deficiencies during regular business hours and the Vendor shall respond back within four (4) hours of notification of planned corrective action; The Vendor shall repair or replace Software, and provide maintenance of the Software in accordance with the Specifications, Terms and Requirements of the Contract.</p>	M	Yes	Standard	<p>FDGS support teams will communicate with the State per the noted timelines for their reported deficiencies.</p> <p>FDGS Tier 1 Call Center Representatives are the first line of contact to research claims, review authorizations and create tickets. These representatives provide minor training and education, and work to address simple or user-related issues. The Tier 1 call center is staffed during standard business hours 8:00 a.m. – 8:00 p.m. Monday through Friday, Eastern Time, excluding holidays, and accesses a language line when there is a need for language translation. Call volumes are counted and measured for effective staffing needs.</p> <p>The Tier 2 Help Desk Specialist Team handles items that require advanced assistance or calls outside of the core hours. Tier 2 Help Desk Specialists have a strong understanding of AuthenticCare and its important compliance requirements for our clients. They have the ability to research reported concerns through application log research, review of Authorizations, Provider agency, Caregiver, Medicaid member, and Service event (visit/claim) files, determine authorization issues and provide in-depth troubleshooting of AuthenticCare software and systems. In some instances, client concerns that reach the Tier 2 Help Desk Specialists are used for training purposes to educate the call center and client alike to promote knowledge sharing.</p>
H4.8	The hosting server for the State shall be available twenty-four (24) hours a day, 7 days a week except for during scheduled maintenance.	M	Yes	Standard	<p>AuthenticCare is available 24 hours by 7 days a week excluding scheduled maintenance. Our virtual server environment and redundancy maximizes availability even during scheduled maintenance windows.</p>
H4.9	A regularly scheduled maintenance window shall be identified (such as weekly, monthly, or quarterly) at which time all relevant server patches and application upgrades shall be applied.	M	Yes	Standard	<p>System maintenance occurs at least monthly and systems are patched in accordance with our Cyber Security standard. Monthly patching occurs based on schedules defined within the FDGS patching portal, with ad hoc patching available if Cyber Team deems a patch to be critical. Once a patch is approved for deployment, FDGS has a dedicated patch team that applies updates and patches.</p> <p>FDGS patch management protocol calls for rigorous pre-deployment testing. Maintenance items are tested in the engineering lab and are promoted and validated in lower environments prior to production deployment.</p>

Exhibit G, Attachment 1
EVV Business and Technical Requirements

H4.10	If The Vendor is unable to meet the uptime requirement, The Vendor shall credit State's account in an amount based upon the following formula: (Total Contract Item Price/365) x Number of Days Contract Item Not Provided. The State must request this credit in writing.	M	Yes	Standard	FDGS has a successful track record of system uptime and agrees to the requirement. FDGS will credit the State's account in an amount based on the provided formula, in writing.
H4.11	The Vendor shall use a change management policy for notification and tracking of change requests as well as critical outages.	M	Yes	Standard	FDGS has a documented Change Management policy that is reviewed during annual third party audits. Change requests are tracked. Our Service Management team will communicate scheduled changes with stakeholders as well as critical outages.
H4.12	A critical outage will be designated when a business function cannot be met by a nonperforming application and there is no work around to the problem.	M	Yes	Standard	FDGS shares this definition of critical outage when there is no workaround for a required business function.
H4.13	The Vendor shall maintain a record of the activities related to repair or maintenance activities performed for the State and shall report quarterly on the following: Server up-time; All change requests implemented, including operating system patches; All critical outages reported including actual issue and resolution; Number of deficiencies reported by class with initial response time as well as time to close.	M	Yes	Standard	This information will be captured and communicated to the State in our monthly operational reports and scorecard.
H4.14	The Vendor will give five business days prior notification to the State Project Manager of all changes/updates and provide the State with training due to the upgrades and changes.	M	Yes	Standard	FDGS will notify and provide training, as needed, to the State at least 5 business days prior to changes/updates, with the exception of immediate repairs need to resolve critical incidents or Class A Deficiencies.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

SUPPORT & MAINTENANCE REQUIREMENTS					
State Requirements			Vendor		
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
SUPPORT & MAINTENANCE REQUIREMENTS					
S1.1	The Vendor's System support and maintenance shall commence upon the Effective Date and extend through the end of the Contract term, and any extensions thereof.	M	Yes	Standard	FDGS support and maintenance for AuthenticCare for DHHS will begin on the effective date and extend through the end of our agreed upon contract term and through any mutual extensions.
S1.2	Maintain the hardware and Software in accordance with the Specifications, terms, and requirements of the Contract, including providing, upgrades and fixes as required.	M	Yes	Standard	FDGS will maintain AuthenticCare and its supporting software and infrastructure in accordance with the agreed upon Contract.
S1.3	Repair Software, or any portion thereof, so that the System operates in accordance with the Specifications, terms, and requirements of the Contract.	M	Yes	Standard	FDGS will maintain AuthenticCare and its supporting software and infrastructure in accordance with the agreed upon Contract.
S1.4	The State shall have unlimited access, via phone or Email, to the Vendor technical support staff between the hours of 8:00am to 5:00pm Monday through Friday EST.	M	Yes	Standard	The AuthenticCare Tier 1 Call Center is accessible through email and telephone 8:00 a.m. to 8:00 p.m. Monday through Friday, Eastern Time, excluding holidays, and accesses a language line when there is a need for language translation.
S1.5	The Vendor response time for support shall conform to the specific deficiency class as described below or as agreed to by the parties: o Class A Deficiency - Software - Critical, does not allow System to operate, no work around, demands immediate action; Written Documentation - missing significant portions of information or unintelligible to State; Non Software - Services were inadequate and require re-performance of the Service. o Class B Deficiency - Software - Important, does not stop operation and/or there is a work around and user can perform tasks; Written Documentation - portions of information are missing but not enough to make the document unintelligible; Non Software - Services were deficient, require reworking, but do not require re-performance of the Service. o Class C Deficiency - Software - minimal, cosmetic in nature, minimal effect on System, low priority and/or user can use System; Written Documentation - minimal changes required and of minor editing nature; Non Software - Services require only minor reworking and do not require re-performance of the Service.	M	Yes	Standard	FDGS will work with the State to define agreed upon response time for each deficiency class. FDGS understands Class A as critical non-operational issue having no work around, Class B as important but does not stop operations or workaround available, and Class C as minimal impact.
S1.6	The Vendor shall make available to the State the latest program updates, general maintenance releases, selected functionality releases, patches, and Documentation that are generally offered to its customers, at no additional cost.	M	Yes	Standard	Generally offered updates to AuthenticCare will be made available to the State at no additional cost.
S1.7	For all maintenance Services calls, The Vendor shall ensure the following information will be collected and maintained: 1) nature of the Deficiency; 2) current status of the Deficiency; 3) action plans, dates, and times; 4) expected and actual completion time; 5) Deficiency resolution information, 6) Resolved by, 7) Identifying number i.e. work order number, 8) Issue identified by;	P	Yes	Standard	The information specified is included within the standard details recorded by our support personnel in our ServiceNow issue management system.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

S1.8	The Vendor must work with the State to identify and troubleshoot potentially large-scale System failures or Deficiencies by collecting the following information: 1) mean time between reported Deficiencies with the Software; 2) diagnosis of the root cause of the problem; and 3) identification of repeat calls or repeat Software problems.	P	Yes	Standard	FDGS uses ServiceNow issue tracking software to record system failures and deficiencies. This system produces reporting used by our support leaders to identify the time between reported issues as well as documenting repeat calls or multiple reported incidents. Major incidents require documentation of a root cause analysis (RCA).
S1.9	As part of the Software maintenance agreement, ongoing software maintenance and support issues, shall be responded to according to the following or as agreed to by the parties: a. Class A Deficiencies - The Vendor shall have available to the State on-call telephone assistance, with issue tracking available to the State, eight (8) hours per day and five (5) days a week with an email / telephone response within two (2) hours of request b. Class B & C Deficiencies - The State shall notify the Vendor of such Deficiencies during regular business hours and the Vendor shall respond back within four (4) hours of notification of planned corrective action; The Vendor shall repair or replace Software, and provide maintenance of the Software in accordance with the Specifications, Terms and Requirements of the Contract; or as agreed between the parties.	M	Yes	Standard	FDGS support teams will communicate with the State per the noted timelines for their reported deficiencies. FDGS Tier 1 Call Center Representatives are the first line of contact to research claims, review authorizations and create tickets. These representatives provide minor training and education, and work to address simple or user-related issues. The Tier 1 call center is staffed during standard business hours 8:00 a.m. – 8:00 p.m. Monday through Friday, Eastern Time, excluding holidays, and accesses a language line when there is a need for language translation. Call volumes are counted and measured for effective staffing needs. The Tier 2 Help Desk Specialist Team handles items that require advanced assistance or calls outside of the core hours. Tier 2 Help Desk Specialists have a strong understanding of AuthentiCare and its important compliance requirements for our clients. They have the ability to research reported concerns through application log research, review of Authorizations, Provider agency, Caregiver, Medicaid member, and Service event (visit/claim) files, determine authorization issues and provide in-depth troubleshooting of AuthentiCare software and systems. In some instances, client concerns that reach the Tier 2 Help Desk Specialists are used for training purposes to educate the call center and client alike to promote knowledge sharing. FDGS support teams will communicate with the State per the noted timelines for their reported deficiencies.
S1.10	The Vendor shall use a change management policy for notification and tracking of change requests as well as critical outages.	M	Yes	Standard	FDGS has a documented Change Management policy that is reviewed during annual third-party audits. Change requests are tracked. Our Service Management team will communicate scheduled changes with stakeholders as well as critical outages.
S1.11	A critical outage will be designated when a business function cannot be met by a nonperforming application and there is no work around to the problem.	M	Yes	Standard	FDGS shares this definition of critical outage when there is no workaround for a required business function.
S1.12	The Vendor shall maintain a record of the activities related to repair or maintenance activities performed for the State and shall report quarterly on the following: All change requests implemented; All critical outages reported including actual issue and resolution; Number of deficiencies reported by class with initial response time as well as time to close.	M	Yes	Standard	FDGS maintains detailed records of all change requests, outages and deficiencies reported and will report this information to the State on a quarterly basis.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

S1.13	A regularly scheduled maintenance window shall be identified (such as weekly, monthly, or quarterly) at which time all relevant server patches and application upgrades shall be applied.	M	Yes	Standard	System maintenance occurs at least monthly and systems are patched in accordance with our Cyber Security standard. Monthly patching occurs based on schedules defined within the FDGS patching portal, with ad hoc patching available if Cyber Team deems a patch to be critical. Once a patch is approved for deployment, FDGS has a dedicated patch team that applies updates and patches. FDGS patch management protocol calls for rigorous pre-deployment testing. Maintenance items are tested in the engineering lab and are promoted and validated in lower environments prior to production deployment.
S1.14	The Vendor shall give five business days prior notification to the State Project Manager of all changes/updates and provide the State with training due to the upgrades and changes.	M	Yes	Standard	FDGS will provide notification at least five business days prior to changes or updates, including associated training materials and training, as needed.
S1.15	The State shall provide the Vendor with a personal secure FTP site to be used by the State for uploading and downloading files if applicable.	M	Yes	Standard	FDGS will work with the State to board our secure file gateway supporting the transfer of files if applicable. The FDGS File Gateway hosted SFTP site is AES 256-bit encrypted according to FIPS 140-2 requirements.
S1.16	Defect fixes will be the responsibility of the Vendor without additional cost to the Department.	M	Yes	Standard	FDGS uses the Business Requirements Document (BRD) to document the New Hampshire system requirements and design. Any defect fixes needed to align to the approved BRD will be completed by our Authenticare teams without additional cost to the Department.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

PROJECT MANAGEMENT					
State Requirements			Vendor		
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
PROJECT MANAGEMENT					
P1.1	Vendor shall participate in an initial kick-off meeting to initiate the Project.	M	Yes	Standard	As a standard part of our implementation process, FDGS initiates collaboration sessions to prepare for and drive the initial project kickoff.
P1.2	Vendor shall provide Project Staff as specified in the RFP.	M	Yes	Standard	FDGS draws resources from a pool of resources that will be dedicated to the project. Supporting resources may be added as needed to meet the requirements in the RFP. Please see Section VI: Qualifications of Key Vendor Staff for our proposed Project Manager and additional key staff.
P1.3	Vendor shall submit a finalized Work Plan within ten (10) days after Contract award and approval by Governor and Council. The Work Plan shall include, without limitation, a detailed description of the Schedule, tasks, Deliverables, milestones/critical events, task dependencies, and payment Schedule. The plan shall be updated no less than every two weeks.	M	Yes	Standard	The FDGS Project Manager will provide a Work Plan within 10 business days after contract award that aligns to the contract timeframe and specified requirements. The Work Plan will include the tasks, deliverables, events and dependencies required as well as those tasks that FDGS, from experience, has used to deliver the EVV solution successfully. The FDGS Project Manager will update the plan at least every two weeks.
P1.4	Vendor shall provide detailed bi-weekly status reports on the progress of the Project, which will include expenses incurred year to date.	M	Yes	Standard	As part of FDGS EVV implementations, FDGS provides weekly status reports inclusive of phase and payment milestones achieved. Additional communications, risks, issues and agreed to detail informing the stakeholders of the health of the project are included in FDGS status reports.
P1.5	All user, technical, and System Documentation as well as Project Schedules, plans, status reports, and correspondence must be maintained as project documentation. (Word and/or Excel formats.)	M	Yes	Standard	The FDGS Project Manager maintains a repository of all project documentation on an internal SharePoint portal as well as an externally shared portal with State access for collaboration and communication purposes. The documentation archives include all project management plans, requirements documents, status reports, schedules, work plans, training guides, and correspondence required by the project and agreed upon by the State. FDGS uses Microsoft Office formats including Word and Excel. The archive is updated regularly as agreed by the project team.
P1.6	Vendor shall provide a full time Project Manager assigned to the DHHS EVV project.	M	Yes	Standard	The full-time project manager proposed is John Cutchin, PMP®. Any changes to the staffing will be defined within the Resource Management subplan of the Project Management Plan and in alignment with contract requirements.
P1.7	The Project Manager will maintain a formal risk register of all identified project risks.	M	Yes	Standard	The FDGS Project Manager maintains for every project a formal Risk Register and Issues List. The high level risk items are listed to drive discussion. The Risk Register is reviewed in status meetings as needed or in ad hoc meetings and distributed and archived on the project SharePoint portal.
P1.8	Vendor's project manager is expected to host meetings with DHHS Subject Matter Experts (SMEs) to review business organization and functions along with the organization, functions and data of existing information systems relevant to this project.	M	Yes	Standard	As part of our standard EVV implementation, the FDGS Project Manager conducts requirements sessions with DHHS subject matter experts to complete the System Integration Plan (SIP) and the Business Requirements Document (BRD). In these sessions the business and organization functions, process and integrations are reviewed and documented.
P1.9	The Vendor's project manager is also expected to host other important meetings, assign contractor staff to those meetings as appropriate and provide an agenda for each meeting.	M	Yes	Standard	The FDGS Project Manager pulls necessary FDGS SMEs from the pool of resources at his disposal from product teams, architecture, business SMEs, operational and training teams to facilitate project success. He hosts necessary meetings both business and technical in nature to gather requirements and facilitate decisions. A standard part of the project management discipline for FDGS is to provide an agenda in advance of meetings as well as minutes within 24 hours.
P1.10	Meeting minutes will be recorded by the contractor and distributed within 24 hours after the meeting. Key decisions along with Closed, Active and Pending issues will be included in this document as well, the Project	M	Yes	Standard	It is part of the FDGS process to provide an agenda for all meetings as well as distribute minutes within 24 hours. Minutes will include action items and issues identified along with agreed upon owners for follow up.

Exhibit G, Attachment 1
EVV Business and Technical Requirements

P1.11	The Project Manager must participate in all other State, provider, and stakeholder meetings as requested by the State.	M	Yes	Standard	In providing for project success, the Project Management Plan identifies the level of participation for the FDGS Project Manager. The FDGS Project Manager participates in State and provider meetings, working closely with the State to support providers and stakeholders. FDGS understands that close collaboration is necessary for the success of the implementation.
P1.12	Deliverable Expectation Documents shall be used to set expectations in preparation for formal deliverable acceptance.	M	Yes	Standard	To properly set expectations, FDGS uses Deliverable Expectation Documents (DEDs) to communicate the required details and content of each non-software deliverable. The DEDs have a place for comments, response, page references and section identification allowing for easily referencing a question and for clarifying any misunderstanding. The result is an improved final deliverable.

New Hampshire Department of Health and Human Services

Exhibit G, Attachment 2



DHHS Agency Compliance Documents

- DHHS Exhibit D, CERTIFICATION REGARDING DRUG-FREE WORKPLACE REQUIREMENTS
- DHHS Exhibit E, CERTIFICATION REGARDING LOBBYING
- DHHS Exhibit F, CERTIFICATION REGARDING DEBARMENT, SUSPENSION, AND OTHER RESPONSIBILITY MATTERS
- DHHS Exhibit G, CERTIFICATION OF COMPLIANCE WITH REQUIREMENTS PERTAINING TO FEDERAL NONDISCRIMINATION, EQUAL TREATMENT OF FAITH-BASED ORGANIZATIONS AND WHISTLEBLOWER PROTECTIONS
- DHHS Exhibit H, CERTIFICATION REGARDING ENVIRONMENTAL TOBACCO SMOKE
- DHHS Exhibit I, HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT BUSINESS ASSOCIATE AGREEMENT
- DHHS Exhibit J, CERTIFICATION REGARDING THE FEDERAL FUNDING ACCOUNTABILITY AND TRANSPARENCY ACT (FFATA) COMPLIANCE
- DHHS Exhibit K, DHHS, INFORMATION SECURITY REQUIREMENTS

**New Hampshire Department of Health and Human Services
Exhibit D**



CERTIFICATION REGARDING DRUG-FREE WORKPLACE REQUIREMENTS

The Vendor identified in Section 1.3 of the General Provisions agrees to comply with the provisions of Sections 5151-5160 of the Drug-Free Workplace Act of 1988 (Pub. L. 100-690, Title V, Subtitle D; 41 U.S.C. 701 et seq.), and further agrees to have the Contractor's representative, as identified in Sections 1.11 and 1.12 of the General Provisions execute the following Certification:

ALTERNATIVE I - FOR GRANTEEES OTHER THAN INDIVIDUALS

**US DEPARTMENT OF HEALTH AND HUMAN SERVICES - CONTRACTORS
US DEPARTMENT OF EDUCATION - CONTRACTORS
US DEPARTMENT OF AGRICULTURE - CONTRACTORS**

This certification is required by the regulations implementing Sections 5151-5160 of the Drug-Free Workplace Act of 1988 (Pub. L. 100-690, Title V, Subtitle D; 41 U.S.C. 701 et seq.). The January 31, 1989 regulations were amended and published as Part II of the May 25, 1990 Federal Register (pages 21681-21691), and require certification by grantees (and by inference, sub-grantees and sub-contractors), prior to award, that they will maintain a drug-free workplace. Section 3017.630(c) of the regulation provides that a grantee (and by inference, sub-grantees and sub-contractors) that is a State may elect to make one certification to the Department in each federal fiscal year in lieu of certificates for each grant during the federal fiscal year covered by the certification. The certificate set out below is a material representation of fact upon which reliance is placed when the agency awards the grant. False certification or violation of the certification shall be grounds for suspension of payments, suspension or termination of grants, or government wide suspension or debarment. Contractors using this form should send it to:

Commissioner
NH Department of Health and Human Services
129 Pleasant Street,
Concord, NH 03301-6505

1. The grantee certifies that it will or will continue to provide a drug-free workplace by:
 - 1.1. Publishing a statement notifying employees that the unlawful manufacture, distribution, dispensing, possession or use of a controlled substance is prohibited in the grantee's workplace and specifying the actions that will be taken against employees for violation of such prohibition;
 - 1.2. Establishing an ongoing drug-free awareness program to inform employees about
 - 1.2.1. The dangers of drug abuse in the workplace;
 - 1.2.2. The grantee's policy of maintaining a drug-free workplace;
 - 1.2.3. Any available drug counseling, rehabilitation, and employee assistance programs; and
 - 1.2.4. The penalties that may be imposed upon employees for drug abuse violations occurring in the workplace;
 - 1.3. Making it a requirement that each employee to be engaged in the performance of the grant be given a copy of the statement required by paragraph (a);
 - 1.4. Notifying the employee in the statement required by paragraph (a) that, as a condition of employment under the grant, the employee will
 - 1.4.1. Abide by the terms of the statement; and
 - 1.4.2. Notify the employer in writing of his or her conviction for a violation of a criminal drug statute occurring in the workplace no later than five calendar days after such conviction;
 - 1.5. Notifying the agency in writing, within ten calendar days after receiving notice under subparagraph 1.4.2 from an employee or otherwise receiving actual notice of such conviction. Employers of convicted employees must provide notice, including position title, to every grant officer on whose grant activity the convicted employee was working, unless the Federal agency

S M

New Hampshire Department of Health and Human Services
Exhibit D



- has designated a central point for the receipt of such notices. Notice shall include the identification number(s) of each affected grant;
- 1.6. Taking one of the following actions, within 30 calendar days of receiving notice under subparagraph 1.4.2, with respect to any employee who is so convicted
 - 1.6.1. Taking appropriate personnel action against such an employee, up to and including termination, consistent with the requirements of the Rehabilitation Act of 1973, as amended; or
 - 1.6.2. Requiring such employee to participate satisfactorily in a drug abuse assistance or rehabilitation program approved for such purposes by a Federal, State, or local health, law enforcement, or other appropriate agency;
 - 1.7. Making a good faith effort to continue to maintain a drug-free workplace through implementation of paragraphs 1.1, 1.2, 1.3, 1.4, 1.5, and 1.6.
2. The grantee may insert in the space provided below the site(s) for the performance of work done in connection with the specific grant.

Place of Performance (street address, city, county, state, zip code) (list each location)

Check ☒ if there are workplaces on file that are not identified here.

Vendor Name: FDGS, Limited Partnership

9/2/2022

Date

Shane McCullough

Name: Shane McCullough

Title: Authorized Signer

New Hampshire Department of Health and Human Services
Exhibit E



CERTIFICATION REGARDING LOBBYING

The Vendor identified in Section 1.3 of the General Provisions agrees to comply with the provisions of Section 319 of Public Law 101-121, Government wide Guidance for New Restrictions on Lobbying, and 31 U.S.C. 1352, and further agrees to have the Contractor's representative, as identified in Sections 1.11 and 1.12 of the General Provisions execute the following Certification:

US DEPARTMENT OF HEALTH AND HUMAN SERVICES - CONTRACTORS
US DEPARTMENT OF EDUCATION - CONTRACTORS
US DEPARTMENT OF AGRICULTURE - CONTRACTORS

Programs (indicate applicable program covered):

- *Temporary Assistance to Needy Families under Title IV-A
- *Child Support Enforcement Program under Title IV-D
- *Social Services Block Grant Program under Title XX
- *Medicaid Program under Title XIX
- *Community Services Block Grant under Title VI
- *Child Care Development Block Grant under Title IV

The undersigned certifies, to the best of his or her knowledge and belief, that:

1. No Federal appropriated funds have been paid or will be paid by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement (and by specific mention sub-grantee or sub-contractor).
2. If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement (and by specific mention sub-grantee or sub-contractor), the undersigned shall complete and submit Standard Form LLL, (Disclosure Form to Report Lobbying, in accordance with its instructions, attached and identified as Standard Exhibit E-1.)
3. The undersigned shall require that the language of this certification be included in the award document for sub-awards at all tiers (including subcontracts, sub-grants, and contracts under grants, loans, and cooperative agreements) and that all sub-recipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by Section 1352, Title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure.

Vendor Name: FDGS, Limited Partnership

9/2/2022

Date

Shane McCullough

Name: Shane McCullough

Title: Authorized Signer

SM

**New Hampshire Department of Health and Human Services
Exhibit F**



**CERTIFICATION REGARDING DEBARMENT, SUSPENSION
AND OTHER RESPONSIBILITY MATTERS**

The Contractor identified in Section 1.3 of the General Provisions agrees to comply with the provisions of Executive Office of the President, Executive Order 12549 and 45 CFR Part 76 regarding Debarment, Suspension, and Other Responsibility Matters, and further agrees to have the Contractor's representative, as identified in Sections 1.11 and 1.12 of the General Provisions execute the following Certification:

INSTRUCTIONS FOR CERTIFICATION

1. By signing and submitting this proposal (contract), the prospective primary participant is providing the certification set out below.
2. The inability of a person to provide the certification required below will not necessarily result in denial of participation in this covered transaction. If necessary, the prospective participant shall submit an explanation of why it cannot provide the certification. The certification or explanation will be considered in connection with the NH Department of Health and Human Services' (DHHS) determination whether to enter into this transaction. However, failure of the prospective primary participant to furnish a certification or an explanation shall disqualify such person from participation in this transaction.
3. The certification in this clause is a material representation of fact upon which reliance was placed when DHHS determined to enter into this transaction. If it is later determined that the prospective primary participant knowingly rendered an erroneous certification, in addition to other remedies available to the Federal Government, DHHS may terminate this transaction for cause or default.
4. The prospective primary participant shall provide immediate written notice to the DHHS agency to whom this proposal (contract) is submitted if at any time the prospective primary participant learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.
5. The terms "covered transaction," "debarred," "suspended," "ineligible," "lower tier covered transaction," "participant," "person," "primary covered transaction," "principal," "proposal," and "voluntarily excluded," as used in this clause, have the meanings set out in the Definitions and Coverage sections of the rules implementing Executive Order 12549: 45 CFR Part 76. See the attached definitions.
6. The prospective primary participant agrees by submitting this proposal (contract) that, should the proposed covered transaction be entered into, it shall not knowingly enter into any lower tier covered transaction with a person who is debarred, suspended, declared ineligible, or voluntarily excluded from participation in this covered transaction, unless authorized by DHHS.
7. The prospective primary participant further agrees by submitting this proposal that it will include the clause titled "Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion - Lower Tier Covered Transactions," provided by DHHS, without modification, in all lower tier covered transactions and in all solicitations for lower tier covered transactions.
8. A participant in a covered transaction may rely upon a certification of a prospective participant in a lower tier covered transaction that it is not debarred, suspended, ineligible, or involuntarily excluded from the covered transaction, unless it knows that the certification is erroneous. A participant may decide the method and frequency by which it determines the eligibility of its principals. Each participant may, but is not required to, check the Nonprocurement List (of excluded parties).
9. Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render in good faith the certification required by this clause. The knowledge and

S M



**New Hampshire Department of Health and Human Services
Exhibit F**

information of a participant is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

10. Except for transactions authorized under paragraph 6 of these instructions, if a participant in a covered transaction knowingly enters into a lower tier covered transaction with a person who is suspended, debarred, ineligible, or voluntarily excluded from participation in this transaction, in addition to other remedies available to the Federal government, DHHS may terminate this transaction for cause or default.

PRIMARY COVERED TRANSACTIONS

11. The prospective primary participant certifies to the best of its knowledge and belief, that it and its principals:
- 11.1. are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any Federal department or agency;
 - 11.2. have not within a three-year period preceding this proposal (contract) been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State or local) transaction or a contract under a public transaction; violation of Federal or State antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;
 - 11.3. are not presently indicted for otherwise criminally or civilly charged by a governmental entity (Federal, State or local) with commission of any of the offenses enumerated in paragraph (I)(b) of this certification; and
 - 11.4. have not within a three-year period preceding this application/proposal had one or more public transactions (Federal, State or local) terminated for cause or default.
12. Where the prospective primary participant is unable to certify to any of the statements in this certification, such prospective participant shall attach an explanation to this proposal (contract).

LOWER TIER COVERED TRANSACTIONS

13. By signing and submitting this lower tier proposal (contract), the prospective lower tier participant, as defined in 45 CFR Part 76, certifies to the best of its knowledge and belief that it and its principals:
- 13.1. are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any federal department or agency.
 - 13.2. where the prospective lower tier participant is unable to certify to any of the above, such prospective participant shall attach an explanation to this proposal (contract).
14. The prospective lower tier participant further agrees by submitting this proposal (contract) that it will include this clause entitled "Certification Regarding Debarment, Suspension, Ineligibility, and Voluntary Exclusion - Lower Tier Covered Transactions," without modification in all lower tier covered transactions and in all solicitations for lower tier covered transactions.

Contractor Name: FDGS, Limited Partnership

9/2/2022

Date

Shane McCullough

Name: Shane McCullough

Title: Authorized Signer

New Hampshire Department of Health and Human Services
Exhibit G



**CERTIFICATION OF COMPLIANCE WITH REQUIREMENTS PERTAINING TO
FEDERAL NONDISCRIMINATION, EQUAL TREATMENT OF FAITH-BASED ORGANIZATIONS AND
WHISTLEBLOWER PROTECTIONS**

The Contractor identified in Section 1.3 of the General Provisions agrees by signature of the Contractor's representative as identified in Sections 1.11 and 1.12 of the General Provisions, to execute the following certification:

Contractor will comply, and will require any subgrantees or subcontractors to comply, with any applicable federal nondiscrimination requirements, which may include:

- the Omnibus Crime Control and Safe Streets Act of 1968 (42 U.S.C. Section 3789d) which prohibits recipients of federal funding under this statute from discriminating, either in employment practices or in the delivery of services or benefits, on the basis of race, color, religion, national origin, and sex. The Act requires certain recipients to produce an Equal Employment Opportunity Plan;
- the Juvenile Justice Delinquency Prevention Act of 2002 (42 U.S.C. Section 5672(b)) which adopts by reference, the civil rights obligations of the Safe Streets Act. Recipients of federal funding under this statute are prohibited from discriminating, either in employment practices or in the delivery of services or benefits, on the basis of race, color, religion, national origin, and sex. The Act includes Equal Employment Opportunity Plan requirements;
- the Civil Rights Act of 1964 (42 U.S.C. Section 2000d, which prohibits recipients of federal financial assistance from discriminating on the basis of race, color, or national origin in any program or activity);
- the Rehabilitation Act of 1973 (29 U.S.C. Section 794), which prohibits recipients of Federal financial assistance from discriminating on the basis of disability, in regard to employment and the delivery of services or benefits, in any program or activity;
- the Americans with Disabilities Act of 1990 (42 U.S.C. Sections 12131-34), which prohibits discrimination and ensures equal opportunity for persons with disabilities in employment, State and local government services, public accommodations, commercial facilities, and transportation;
- the Education Amendments of 1972 (20 U.S.C. Sections 1681, 1683, 1685-86), which prohibits discrimination on the basis of sex in federally assisted education programs;
- the Age Discrimination Act of 1975 (42 U.S.C. Sections 6106-07), which prohibits discrimination on the basis of age in programs or activities receiving Federal financial assistance. It does not include employment discrimination;
- 28 C.F.R. pt. 31 (U.S. Department of Justice Regulations – OJJDP Grant Programs); 28 C.F.R. pt. 42 (U.S. Department of Justice Regulations – Nondiscrimination, Equal Employment Opportunity, Policies and Procedures); Executive Order No. 13279 (equal protection of the laws for faith-based and community organizations); Executive Order No. 13559, which provide fundamental principles and policy-making criteria for partnerships with faith-based and neighborhood organizations;
- 28 C.F.R. pt. 38 (U.S. Department of Justice Regulations – Equal Treatment for Faith-Based Organizations); and Whistleblower protections 41 U.S.C. §4712 and The National Defense Authorization Act (NDAA) for Fiscal Year 2013 (Pub. L. 112-239, enacted January 2, 2013) the Pilot Program for Enhancement of Contract Employee Whistleblower Protections, which protects employees against reprisal for certain whistle blowing activities in connection with federal grants and contracts.

The certificate set out below is a material representation of fact upon which reliance is placed when the agency awards the grant. False certification or violation of the certification shall be grounds for suspension of payments, suspension or termination of grants, or government wide suspension or debarment.

Exhibit G

Contractor Initials

S M

Certification of Compliance with requirements pertaining to Federal Nondiscrimination, Equal Treatment of Faith-Based Organizations and Whistleblower protections

New Hampshire Department of Health and Human Services
Exhibit G



In the event a Federal or State court or Federal or State administrative agency makes a finding of discrimination after a due process hearing on the grounds of race, color, religion, national origin, or sex against a recipient of funds, the recipient will forward a copy of the finding to the Office for Civil Rights, to the applicable contracting agency or division within the Department of Health and Human Services, and to the Department of Health and Human Services Office of the Ombudsman.

The Contractor identified in Section 1.3 of the General Provisions agrees by signature of the Contractor's representative as identified in Sections 1.11 and 1.12 of the General Provisions, to execute the following certification:

- I. By signing and submitting this proposal (contract) the Contractor agrees to comply with the provisions indicated above.

Contractor Name: FDGS, Limited Partnership

9/2/2022

Date

Shane McCullough

Name: Shane McCullough

Title: Authorized Signer

Exhibit G

Contractor Initials

SM

Certification of Compliance with requirements pertaining to Federal Nondiscrimination, Equal Treatment of Faith-Based Organizations and Whistleblower protections

New Hampshire Department of Health and Human Services
Exhibit H



CERTIFICATION REGARDING ENVIRONMENTAL TOBACCO SMOKE

Public Law 103-227, Part C - Environmental Tobacco Smoke, also known as the Pro-Children Act of 1994 (Act), requires that smoking not be permitted in any portion of any indoor facility owned or leased or contracted for by an entity and used routinely or regularly for the provision of health, day care, education, or library services to children under the age of 18, if the services are funded by Federal programs either directly or through State or local governments, by Federal grant, contract, loan, or loan guarantee. The law does not apply to children's services provided in private residences, facilities funded solely by Medicare or Medicaid funds, and portions of facilities used for inpatient drug or alcohol treatment. Failure to comply with the provisions of the law may result in the imposition of a civil monetary penalty of up to \$1000 per day and/or the imposition of an administrative compliance order on the responsible entity.

The Contractor identified in Section 1.3 of the General Provisions agrees, by signature of the Contractor's representative as identified in Section 1.11 and 1.12 of the General Provisions, to execute the following certification:

1. By signing and submitting this contract, the Contractor agrees to make reasonable efforts to comply with all applicable provisions of Public Law 103-227, Part C, known as the Pro-Children Act of 1994.

Contractor Name: FDGS, Limited Partnership

9/2/2022

Date

Shane McCullough

Name: Shane McCullough

Title: Authorized Signer



New Hampshire Department of Health and Human Services

Exhibit I

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT BUSINESS ASSOCIATE AGREEMENT

The Contractor identified in Section 1.3 of the General Provisions of the Agreement agrees to comply with the Health Insurance Portability and Accountability Act, Public Law 104-191 and with the Standards for Privacy and Security of Individually Identifiable Health Information, 45 CFR Parts 160 and 164 applicable to business associates. As defined herein, "Business Associate" shall mean the Contractor and subcontractors and agents of the Contractor that receive, use or have access to protected health information under this Agreement and "Covered Entity" shall mean the State of New Hampshire, Department of Health and Human Services.

(1) Definitions.

- a. "Breach" shall have the same meaning as the term "Breach" in section 164.402 of Title 45, Code of Federal Regulations.
- b. "Business Associate" has the meaning given such term in section 160.103 of Title 45, Code of Federal Regulations.
- c. "Covered Entity" has the meaning given such term in section 160.103 of Title 45, Code of Federal Regulations.
- d. "Designated Record Set" shall have the same meaning as the term "designated record set" in 45 CFR Section 164.501.
- e. "Data Aggregation" shall have the same meaning as the term "data aggregation" in 45 CFR Section 164.501.
- f. "Health Care Operations" shall have the same meaning as the term "health care operations" in 45 CFR Section 164.501.
- g. "HITECH Act" means the Health Information Technology for Economic and Clinical Health Act, Title XIII, Subtitle D, Part 1 & 2 of the American Recovery and Reinvestment Act of 2009.
- h. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 and the Standards for Privacy and Security of Individually Identifiable Health Information, 45 CFR Parts 160, 162 and 164 and amendments thereto.
- i. "Individual" shall have the same meaning as the term "individual" in 45 CFR Section 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR Section 164.501(g).
- j. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164, promulgated under HIPAA by the United States Department of Health and Human Services.
- k. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR Section 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

S M

3/2014

Exhibit I
Health Insurance Portability Act
Business Associate Agreement
Page 1 of 6

Contractor Initials _____

9/2/2022
Date _____



New Hampshire Department of Health and Human Services

Exhibit I

- l. "Required by Law" shall have the same meaning as the term "required by law" in 45 CFR Section 164.103.
- m. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his/her designee.
- n. "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Part 164, Subpart C, and amendments thereto.
- o. "Unsecured Protected Health Information" means protected health information that is not secured by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.
- p. Other Definitions - All terms not otherwise defined herein shall have the meaning established under 45 C.F.R. Parts 160, 162 and 164, as amended from time to time, and the HITECH Act.

(2) Business Associate Use and Disclosure of Protected Health Information.

- a. Business Associate shall not use, disclose, maintain or transmit Protected Health Information (PHI) except as reasonably necessary to provide the services outlined under Exhibit A of the Agreement. Further, Business Associate, including but not limited to all its directors, officers, employees and agents, shall not use, disclose, maintain or transmit PHI in any manner that would constitute a violation of the Privacy and Security Rule.
- b. Business Associate may use or disclose PHI:
- I. For the proper management and administration of the Business Associate;
 - II. As required by law, pursuant to the terms set forth in paragraph d. below; or
 - III. For data aggregation purposes for the health care operations of Covered Entity.
- c. To the extent Business Associate is permitted under the Agreement to disclose PHI to a third party, Business Associate must obtain, prior to making any such disclosure, (i) reasonable assurances from the third party that such PHI will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the third party; and (ii) an agreement from such third party to notify Business Associate, in accordance with the HIPAA Privacy, Security, and Breach Notification Rules of any breaches of the confidentiality of the PHI, to the extent it has obtained knowledge of such breach.
- d. The Business Associate shall not, unless such disclosure is reasonably necessary to provide services under Exhibit A of the Agreement, disclose any PHI in response to a request for disclosure on the basis that it is required by law, without first notifying Covered Entity so that Covered Entity has an opportunity to object to the disclosure and to seek appropriate relief. If Covered Entity objects to such disclosure, the Business

S M



New Hampshire Department of Health and Human Services

Exhibit I

Associate shall refrain from disclosing the PHI until Covered Entity has exhausted all remedies.

- e. If the Covered Entity notifies the Business Associate that Covered Entity has agreed to be bound by additional restrictions over and above those uses or disclosures or security safeguards of PHI pursuant to the Privacy and Security Rule, the Business Associate shall be bound by such additional restrictions and shall not disclose PHI in violation of such additional restrictions and shall abide by any additional security safeguards.

(3) Obligations and Activities of Business Associate.

- a. The Business Associate shall notify the Covered Entity's Privacy Officer immediately after the Business Associate becomes aware of any use or disclosure of protected health information not provided for by the Agreement including breaches of unsecured protected health information and/or any security incident that may have an impact on the protected health information of the Covered Entity.
- b. The Business Associate shall immediately perform a risk assessment when it becomes aware of any of the above situations. The risk assessment shall include, but not be limited to:
- o The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
 - o The unauthorized person used the protected health information or to whom the disclosure was made;
 - o Whether the protected health information was actually acquired or viewed
 - o The extent to which the risk to the protected health information has been mitigated.

The Business Associate shall complete the risk assessment within 48 hours of the breach and immediately report the findings of the risk assessment in writing to the Covered Entity.

- c. The Business Associate shall comply with all sections of the Privacy, Security, and Breach Notification Rule.
- d. Business Associate shall make available all of its internal policies and procedures, books and records relating to the use and disclosure of PHI received from, or created or received by the Business Associate on behalf of Covered Entity to the Secretary for purposes of determining Covered Entity's compliance with HIPAA and the Privacy and Security Rule.
- e. Business Associate shall require all of its business associates that receive, use or have access to PHI under the Agreement, to agree in writing to adhere to the same restrictions and conditions on the use and disclosure of PHI contained herein, including the duty to return or destroy the PHI as provided under Section 3 (I). The Covered Entity shall be considered a direct third party beneficiary of the Contractor's business associate agreements with Contractor's intended business associates, who will be receiving PHI



New Hampshire Department of Health and Human Services

Exhibit I

pursuant to this Agreement, with rights of enforcement and indemnification from such business associates who shall be governed by standard Paragraph #13 of the standard contract provisions (P-37) of this Agreement for the purpose of use and disclosure of protected health information.

- f. Within five (5) business days of receipt of a written request from Covered Entity, Business Associate shall make available during normal business hours at its offices all records, books, agreements, policies and procedures relating to the use and disclosure of PHI to the Covered Entity, for purposes of enabling Covered Entity to determine Business Associate's compliance with the terms of the Agreement.
- g. Within ten (10) business days of receiving a written request from Covered Entity, Business Associate shall provide access to PHI in a Designated Record Set to the Covered Entity, or as directed by Covered Entity, to an individual in order to meet the requirements under 45 CFR Section 164.524.
- h. Within ten (10) business days of receiving a written request from Covered Entity for an amendment of PHI or a record about an individual contained in a Designated Record Set, the Business Associate shall make such PHI available to Covered Entity for amendment and incorporate any such amendment to enable Covered Entity to fulfill its obligations under 45 CFR Section 164.526.
- i. Business Associate shall document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 CFR Section 164.528.
- j. Within ten (10) business days of receiving a written request from Covered Entity for a request for an accounting of disclosures of PHI, Business Associate shall make available to Covered Entity such information as Covered Entity may require to fulfill its obligations to provide an accounting of disclosures with respect to PHI in accordance with 45 CFR Section 164.528.
- k. In the event any individual requests access to, amendment of, or accounting of PHI directly from the Business Associate, the Business Associate shall within two (2) business days forward such request to Covered Entity. Covered Entity shall have the responsibility of responding to forwarded requests. However, if forwarding the individual's request to Covered Entity would cause Covered Entity or the Business Associate to violate HIPAA and the Privacy and Security Rule, the Business Associate shall instead respond to the individual's request as required by such law and notify Covered Entity of such response as soon as practicable.
- l. Within ten (10) business days of termination of the Agreement, for any reason, the Business Associate shall return or destroy, as specified by Covered Entity, all PHI received from, or created or received by the Business Associate in connection with the Agreement, and shall not retain any copies or back-up tapes of such PHI. If return or destruction is not feasible, or the disposition of the PHI has been otherwise agreed to in the Agreement, Business Associate shall continue to extend the protections of the Agreement, to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate

3/2014

Contractor Initials S M

9/2/2022
Date



New Hampshire Department of Health and Human Services

Exhibit I

Associate maintains such PHI. If Covered Entity, in its sole discretion, requires that the Business Associate destroy any or all PHI, the Business Associate shall certify to Covered Entity that the PHI has been destroyed.

(4) Obligations of Covered Entity

- a. Covered Entity shall notify Business Associate of any changes or limitation(s) in its Notice of Privacy Practices provided to individuals in accordance with 45 CFR Section 164.520, to the extent that such change or limitation may affect Business Associate's use or disclosure of PHI.
- b. Covered Entity shall promptly notify Business Associate of any changes in, or revocation of permission provided to Covered Entity by individuals whose PHI may be used or disclosed by Business Associate under this Agreement, pursuant to 45 CFR Section 164.506 or 45 CFR Section 164.508.
- c. Covered entity shall promptly notify Business Associate of any restrictions on the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

(5) Termination for Cause

In addition to Paragraph 10 of the standard terms and conditions (P-37) of this Agreement the Covered Entity may immediately terminate the Agreement upon Covered Entity's knowledge of a breach by Business Associate of the Business Associate Agreement set forth herein as Exhibit I. The Covered Entity may either immediately terminate the Agreement or provide an opportunity for Business Associate to cure the alleged breach within a timeframe specified by Covered Entity. If Covered Entity determines that neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

(6) Miscellaneous

- a. Definitions and Regulatory References. All terms used, but not otherwise defined herein, shall have the same meaning as those terms in the Privacy and Security Rule, amended from time to time. A reference in the Agreement, as amended to include this Exhibit I, to a Section in the Privacy and Security Rule means the Section as in effect or as amended.
- b. Amendment. Covered Entity and Business Associate agree to take such action as is necessary to amend the Agreement, from time to time as is necessary for Covered Entity to comply with the changes in the requirements of HIPAA, the Privacy and Security Rule, and applicable federal and state law.
- c. Data Ownership. The Business Associate acknowledges that it has no ownership rights with respect to the PHI provided by or created on behalf of Covered Entity.
- d. Interpretation. The parties agree that any ambiguity in the Agreement shall be resolved to permit Covered Entity to comply with HIPAA, the Privacy and Security Rule. *S M*

3/2014

Contractor Initials *S M*

9/2/2022
Date



New Hampshire Department of Health and Human Services

Exhibit I

- e. Segregation. If any term or condition of this Exhibit I or the application thereof to any person(s) or circumstance is held invalid, such invalidity shall not affect other terms or conditions which can be given effect without the invalid term or condition; to this end the terms and conditions of this Exhibit I are declared severable.
- f. Survival. Provisions in this Exhibit I regarding the use and disclosure of PHI, return or destruction of PHI, extensions of the protections of the Agreement in section (3) I, the defense and indemnification provisions of section (3) e and Paragraph 13 of the standard terms and conditions (P-37), shall survive the termination of the Agreement.

IN WITNESS WHEREOF, the parties hereto have duly executed this Exhibit I.

Department of Health and Human Services

The State

Melissa Hardy

Signature of Authorized Representative

Melissa Hardy

Name of Authorized Representative
Director, DLTSS

Title of Authorized Representative

9/2/2022

Date

FDGS, Limited Partnership

Name of the Contractor

Shane McCullough

Signature of Authorized Representative

Shane McCullough

Name of Authorized Representative

Authorized Signer

Title of Authorized Representative

9/2/2022

Date

**New Hampshire Department of Health and Human Services
Exhibit J**



**CERTIFICATION REGARDING THE FEDERAL FUNDING ACCOUNTABILITY AND TRANSPARENCY
ACT (FFATA) COMPLIANCE**

The Federal Funding Accountability and Transparency Act (FFATA) requires prime awardees of individual Federal grants equal to or greater than \$25,000 and awarded on or after October 1, 2010, to report on data related to executive compensation and associated first-tier sub-grants of \$25,000 or more. If the initial award is below \$25,000 but subsequent grant modifications result in a total award equal to or over \$25,000, the award is subject to the FFATA reporting requirements, as of the date of the award.

In accordance with 2 CFR Part 170 (Reporting Subaward and Executive Compensation Information), the Department of Health and Human Services (DHHS) must report the following information for any subaward or contract award subject to the FFATA reporting requirements:

1. Name of entity
2. Amount of award
3. Funding agency
4. NAICS code for contracts / CFDA program number for grants
5. Program source
6. Award title descriptive of the purpose of the funding action
7. Location of the entity
8. Principle place of performance
9. Unique identifier of the entity (UEI #)
10. Total compensation and names of the top five executives if:
 - 10.1. More than 80% of annual gross revenues are from the Federal government, and those revenues are greater than \$25M annually and
 - 10.2. Compensation information is not already available through reporting to the SEC.

Prime grant recipients must submit FFATA required data by the end of the month, plus 30 days, in which the award or award amendment is made.

The Contractor identified in Section 1.3 of the General Provisions agrees to comply with the provisions of The Federal Funding Accountability and Transparency Act, Public Law 109-282 and Public Law 110-252, and 2 CFR Part 170 (Reporting Subaward and Executive Compensation Information), and further agrees to have the Contractor's representative, as identified in Sections 1.11 and 1.12 of the General Provisions execute the following Certification:

The below named Contractor agrees to provide needed information as outlined above to the NH Department of Health and Human Services and to comply with all applicable provisions of the Federal Financial Accountability and Transparency Act.

Contractor Name: FDGS, Limited Partnership

9/2/2022

Date

Shane McCullough

Name: Shane McCullough

Title: Authorized Signer



**New Hampshire Department of Health and Human Services
Exhibit J**

FORM A

As the Contractor identified in Section 1.3 of the General Provisions, I certify that the responses to the below listed questions are true and accurate.

1. The UEI (SAM.gov) number for your entity is: QXQHTGUR54Q1
2. In your business or organization's preceding completed fiscal year, did your business or organization receive (1) 80 percent or more of your annual gross revenue in U.S. federal contracts, subcontracts, loans, grants, sub-grants, and/or cooperative agreements; and (2) \$25,000,000 or more in annual gross revenues from U.S. federal contracts, subcontracts, loans, grants, subgrants, and/or cooperative agreements?

 NO X YES

If the answer to #2 above is NO, stop here

If the answer to #2 above is YES, please answer the following:

3. Does the public have access to information about the compensation of the executives in your business or organization through periodic reports filed under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m(a), 78o(d)) or section 6104 of the Internal Revenue Code of 1986?

 NO X YES

If the answer to #3 above is YES, stop here

If the answer to #3 above is NO, please answer the following:

4. The names and compensation of the five most highly compensated officers in your business or organization are as follows:

Name: _____	Amount: _____
Name: _____	Amount: _____
Name: _____	Amount: _____
Name: _____	Amount: _____
Name: _____	Amount: _____

New Hampshire Department of Health and Human Services

Exhibit K

DHHS Information Security Requirements



A. Definitions

The following terms may be reflected and have the described meaning in this document:

1. "Breach" means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic. With regard to Protected Health Information, "Breach" shall have the same meaning as the term "Breach" in section 164.402 of Title 45, Code of Federal Regulations.

2. "Computer Security Incident" shall have the same meaning "Computer Security Incident" in section two (2) of NIST Publication 800-61, Computer Security Incident Handling Guide, National Institute of Standards and Technology, U.S. Department of Commerce.

3. "Confidential Information" or "Confidential Data" means all confidential information disclosed by one party to the other such as all medical, health, financial, public assistance benefits and personal information including without limitation, Substance Abuse Treatment Records, Case Records, Protected Health Information and Personally Identifiable Information.

Confidential Information also includes any and all information owned or managed by the State of NH - created, received from or on behalf of the Department of Health and Human Services (DHHS) or accessed in the course of performing contracted services - of which collection, disclosure, protection, and disposition is governed by state or federal law or regulation. This information includes, but is not limited to Protected Health Information (PHI), Personal Information (PI), Personal Financial Information (PFI), Federal Tax Information (FTI), Social Security Numbers (SSN), Payment Card Industry (PCI), and or other sensitive and confidential information.

4. "End User" means any person or entity (e.g., contractor, contractor's employee, business associate, subcontractor, other downstream user, etc.) that receives DHHS data or derivative data in accordance with the terms of this Contract.
5. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder.
6. "Incident" means an act that potentially violates an explicit or implied security policy, which includes attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent. Incidents include the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, and misrouting of physical or electronic

New Hampshire Department of Health and Human Services

Exhibit K

DHHS Information Security Requirements



mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification or destruction.

7. "Open Wireless Network" means any network or segment of a network that is not designated by the State of New Hampshire's Department of Information Technology or delegate as a protected network (designed, tested, and approved, by means of the State, to transmit) will be considered an open network and not adequately secure for the transmission of unencrypted PI, PFI, PHI or confidential DHHS data.
8. "Personal Information" (or "PI") means information which can be used to distinguish or trace an individual's identity, such as their name, social security number, personal information as defined in New Hampshire RSA 359-C:19, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
9. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, promulgated under HIPAA by the United States Department of Health and Human Services.
10. "Protected Health Information" (or "PHI") has the same meaning as provided in the definition of "Protected Health Information" in the HIPAA Privacy Rule at 45 C.F.R. § 160.103.
11. "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Part 164, Subpart C, and amendments thereto.
12. "Unsecured Protected Health Information" means Protected Health Information that is not secured by a technology standard that renders Protected Health Information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

I. RESPONSIBILITIES OF DHHS AND THE CONTRACTOR

A. Business Use and Disclosure of Confidential Information.

1. The Contractor must not use, disclose, maintain or transmit Confidential Information except as reasonably necessary as outlined under this Contract. Further, Contractor, including but not limited to all its directors, officers, employees and agents, must not use, disclose, maintain or transmit PHI in any manner that would constitute a violation of the Privacy and Security Rule.
2. The Contractor must not disclose any Confidential Information in response to a

New Hampshire Department of Health and Human Services

Exhibit K

DHHS Information Security Requirements



request for disclosure on the basis that it is required by law, in response to a subpoena, etc., without first notifying DHHS so that DHHS has an opportunity to consent or object to the disclosure.

3. If DHHS notifies the Contractor that DHHS has agreed to be bound by additional restrictions over and above those uses or disclosures or security safeguards of PHI pursuant to the Privacy and Security Rule, the Contractor must be bound by such additional restrictions and must not disclose PHI in violation of such additional restrictions and must abide by any additional security safeguards.
4. The Contractor agrees that DHHS Data or derivative there from disclosed to an End User must only be used pursuant to the terms of this Contract.
5. The Contractor agrees DHHS Data obtained under this Contract may not be used for any other purposes that are not indicated in this Contract.
6. The Contractor agrees to grant access to the data to the authorized representatives of DHHS for the purpose of inspecting to confirm compliance with the terms of this Contract.

II. METHODS OF SECURE TRANSMISSION OF DATA

1. Application Encryption. If End User is transmitting DHHS data containing Confidential Data between applications, the Contractor attests the applications have been evaluated by an expert knowledgeable in cyber security and that said application's encryption capabilities ensure secure transmission via the internet.
2. Computer Disks and Portable Storage Devices. End User may not use computer disks or portable storage devices, such as a thumb drive, as a method of transmitting DHHS data.
3. Encrypted Email. End User may only employ email to transmit Confidential Data if email is encrypted and being sent to and being received by email addresses of persons authorized to receive such information.
4. Encrypted Web Site. If End User is employing the Web to transmit Confidential Data, the secure socket layers (SSL) must be used and the web site must be secure. SSL encrypts data transmitted via a Web site.
5. File Hosting Services, also known as File Sharing Sites. End User may not use file hosting services, such as Dropbox or Google Cloud Storage, to transmit Confidential Data.
6. Ground Mail Service. End User may only transmit Confidential Data via *certified* ground mail within the continental U.S. and when sent to a named individual.
7. Laptops and PDA. If End User is employing portable devices to transmit Confidential Data said devices must be encrypted and password-protected.
8. Open Wireless Networks.

New Hampshire Department of Health and Human Services

Exhibit K

DHHS Information Security Requirements



- . Contractor may not transmit Confidential Data via an open wireless network, unless employing a secure method of transmission or remote access, which complies with the terms and conditions of this Information Security Requirements Exhibit, such as a virtual private network (VPN).
9. Remote User Communication. If Contractor is employing remote communication to access or transmit Confidential Data, a secure method of transmission or remote access, which complies with the terms and conditions of this Information Security Requirements Exhibit, must be used, such as a virtual private network (VPN).
 10. SSH File Transfer Protocol (SFTP), also known as Secure File Transfer Protocol. If End User is employing an SFTP to transmit Confidential Data, End User will structure the Folder and access privileges to prevent inappropriate disclosure of information. SFTP folders and sub-folders used for transmitting Confidential Data will be coded for 24-hour auto-deletion cycle (i.e. Confidential Data will be deleted every 24 hours).
 11. Wireless Devices. If End User is transmitting Confidential Data via wireless devices, all data must be encrypted to prevent inappropriate disclosure of information.

III. RETENTION AND DISPOSITION OF IDENTIFIABLE RECORDS

The Contractor will only retain the data and any derivative of the data for the duration of this Contract. After such time, the Contractor will have 30 days to destroy the data and any derivative in whatever form it may exist, unless, otherwise required by law or permitted under this Contract. To this end, the parties must:

A. Retention

1. The Contractor agrees it will not store, transfer or process data collected in connection with the services rendered under this Contract outside of the United States. This physical location requirement shall also apply in the implementation of cloud computing, cloud service or cloud storage capabilities, and includes backup data and Disaster Recovery locations.
2. The Contractor agrees to ensure proper security monitoring capabilities are in place to detect potential security events that can impact State of NH systems and/or Department confidential information for contractor provided systems.
3. The Contractor agrees to provide security awareness and education for its End Users in support of protecting Department confidential information.
4. The Contractor agrees to retain all electronic and hard copies of Confidential Data in a secure location and identified in section IV. A.2
5. The Contractor agrees Data stored in a Cloud must be in a FedRAMP, HITECH, government or HIPAA compliant cloud solution, appropriate for the type of data stored and/or processed or transmitted, and comply with all applicable statutes and regulations regarding the privacy and security, including all requirements contained within this Exhibit. Further, Contractor will test and ensure the HIPAA compliant solution is correctly architected to avoid configuration errors that would leave

New Hampshire Department of Health and Human Services

Exhibit K

DHHS Information Security Requirements



protected health information (PHI) or personally identifiable information (PII) unprotected and accessible by unauthorized individuals or vulnerable to insider threat.

All Contractor or End User controlled servers and devices must follow the hardening standards as outline in NIST. As well as current, updated, and maintained anti-malware utilities (e.g. anti-viral, anti-hacker, anti-spam, anti-spyware). The environment, as a whole, must have intrusion-detection services and intrusion protection services, as well as, firewall protection.

6. The Contractor agrees to and ensures its complete cooperation with the State's Chief Information Officer in the detection of any security vulnerability of the hosting infrastructure.

B. Disposition

1. If the Contractor will maintain any Confidential Information on its systems (or its sub-contractor systems), the Contractor will maintain a documented process for securely disposing of such data upon request or contract termination; and will obtain written certification for any State of New Hampshire data destroyed by the Contractor or any subcontractors as a part of ongoing, emergency, and or disaster recovery operations. When no longer in use, electronic media containing State of New Hampshire data shall be rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion and media sanitization, or otherwise physically destroying the media (for example, degaussing) as described in NIST Special Publication 800-88, Rev 1, Guidelines for Media Sanitization, National Institute of Standards and Technology, U. S. Department of Commerce. The Contractor will document and certify in writing at time of the data destruction, and will provide written certification to the Department upon request. The written certification will include all details necessary to demonstrate data has been properly destroyed and validated. Where applicable, regulatory and professional standards for retention requirements will be jointly evaluated by the State and Contractor prior to destruction.
2. Unless otherwise specified, within thirty (30) days of the termination of this Contract, Contractor agrees to destroy all hard copies of Confidential Data using a secure method such as shredding.
3. Unless otherwise specified, within thirty (30) days of the termination of this Contract, Contractor agrees to completely destroy all electronic Confidential Data by means of data erasure, also known as secure data wiping.

IV. PROCEDURES FOR SECURITY

- A. Contractor agrees to safeguard the DHHS Data received under this Contract, and any derivative data or files, as follows:

1. The Contractor will maintain proper security controls to protect Department confidential information collected, processed, managed, and/or stored in the delivery of contracted services.

New Hampshire Department of Health and Human Services

Exhibit K

DHHS Information Security Requirements



2. The Contractor will maintain policies and procedures to protect Department confidential information throughout the information lifecycle, where applicable, (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e., tape, disk, paper, etc.).
3. The Contractor will maintain appropriate authentication and access controls to contractor systems that collect, transmit, or store Department confidential information where applicable.
4. The Contractor will ensure proper security monitoring capabilities are in place to detect potential security events that can impact State of NH systems and/or Department confidential information for contractor provided systems.
5. If the Contractor has adopted a "Bring Your Own Device (BYOD)" policy said policy shall require the Contractor to provide its remote workforce with a secure environment via Desktop as a Service for their personal devices to access all systems for processing. The Contractor shall ensure that all devices meet the security requirements of this and contract and that the following security requirements are in place prior to personal devices being used for this contract:
 - a. Encrypt each personal devices end-to-end
 - b. Data collected through this contract shall not be stored in any format on personal devices;
 - c. Scan each personal device to ensure the device follows the same security protocols as the Contractor-owned devices; All personal devices will adhere the security requirements set forth in this exhibit;
 - d. Employ on-demand scanners for each device to initiate a full scan at any time to check the entire personal device (files, folders, programs, etc., including removable storage devices;
 - e. All personal devices are recorded, and trackable, in the Contractor's asset inventories and risk assessments; and
 - f. Written exception for personal device usage by NH DHHS Information Security has been provided.
6. The Contractor will provide regular security awareness and education for its End Users in support of protecting Department confidential information.
7. If the Contractor will be sub-contracting any core functions of the engagement supporting the services for State of New Hampshire, the Contractor will maintain a program of an internal process or processes that defines specific security expectations, and monitoring compliance to security requirements that at a minimum match those for the Contractor, including breach notification requirements. The Contractor will work with the Department to sign and comply with all applicable State of New Hampshire and Department system access and authorization policies and procedures, systems access forms, and computer use agreements as part of obtaining and maintaining access to any Department system(s). Agreements will be completed and signed by the Contractor and any applicable sub-contractors prior to system access being authorized.
8. If the Department determines the Contractor is a Business Associate pursuant to 45 CFR 160.103, the Contractor will execute a HIPAA Business Associate Agreement

New Hampshire Department of Health and Human Services

Exhibit K

DHHS Information Security Requirements



- (BAA) with the Department and is responsible for maintaining compliance with the agreement.
9. The Contractor will work with the Department at its request to complete a System Management Survey. The purpose of the survey is to enable the Department and Contractor to monitor for any changes in risks, threats, and vulnerabilities that may occur over the life of the Contractor engagement. The survey will be completed annually, or an alternate time frame at the Departments discretion with agreement by the Contractor, or the Department may request the survey be completed when the scope of the engagement between the Department and the Contractor changes.
 10. The Contractor will not store, knowingly or unknowingly, any State of New Hampshire or Department data offshore or outside the boundaries of the United States unless prior express written consent is obtained from the Information Security Office leadership member within the Department.
 11. Data Security Breach Liability. In the event of any security breach Contractor shall make efforts to investigate the causes of the breach, promptly take measures to prevent future breach and minimize any damage or loss resulting from the breach. The State shall recover from the Contractor all costs of response and recovery from the breach, including but not limited to: credit monitoring services, mailing costs and costs associated with website and telephone call center services necessary due to the breach. Contractor shall bear all costs associated with system downtime, system or data breach, data loss or misuse as a result of its Bring Your Own Device (BYOD) Policy.
 12. Contractor must, comply with all applicable statutes and regulations regarding the privacy and security of Confidential Information, and must in all other respects maintain the privacy and security of PI and PHI at a level and scope that is not less than the level and scope of requirements applicable to federal agencies, including, but not limited to, provisions of the Privacy Act of 1974 (5 U.S.C. § 552a), DHHS Privacy Act Regulations (45 C.F.R. §5b), HIPAA Privacy and Security Rules (45 C.F.R. Parts 160 and 164) that govern protections for individually identifiable health information and as applicable under State law.
 13. Contractor agrees to establish and maintain appropriate administrative, technical, and physical safeguards to protect the confidentiality of the Confidential Data and to prevent unauthorized use or access to it. The safeguards must provide a level and scope of security that is not less than the level and scope of security requirements established by the State of New Hampshire, Department of Information Technology. Refer to Vendor Resources/Procurement at <https://www.nh.gov/doit/vendor/index.htm> for the Department of Information Technology policies, guidelines, standards, and procurement information relating to vendors.
 14. Contractor agrees to maintain a documented breach notification and incident response process. The Contractor will notify the State's Privacy Officer and the State's Security Officer of any security breach immediately, at the email addresses provided in Section VI. This includes a confidential information breach, computer security incident, or suspected breach which affects or includes any State of New Hampshire systems that

New Hampshire Department of Health and Human Services

Exhibit K

DHHS Information Security Requirements



connect to the State of New Hampshire network.

15. Contractor must restrict access to the Confidential Data obtained under this Contract to only those authorized End Users who need such DHHS Data to perform their official duties in connection with purposes identified in this Contract.
16. The Contractor must ensure that all End Users:
 - a. comply with such safeguards as referenced in Section IV A. above, implemented to protect Confidential Information that is furnished by DHHS under this Contract from loss, theft or inadvertent disclosure.
 - b. safeguard this information at all times.
 - c. ensure that laptops and other electronic devices/media containing PHI, PI, or PFI are encrypted and password-protected.
 - d. send emails containing Confidential Information only if encrypted and being sent to and being received by email addresses of persons authorized to receive such information.
 - e. limit disclosure of the Confidential Information to the extent permitted by law.
 - f. Confidential Information received under this Contract and individually identifiable data derived from DHHS Data, must be stored in an area that is physically and technologically secure from access by unauthorized persons during duty hours as well as non-duty hours (e.g., door locks, card keys, biometric identifiers, etc.).
 - g. only authorized End Users may transmit the Confidential Data, including any derivative files containing personally identifiable information, and in all cases, such data must be encrypted at all times when in transit, at rest, or when stored on portable media as required in section IV above.
 - h. in all other instances Confidential Data must be maintained, used and disclosed using appropriate safeguards, as determined by a risk-based assessment of the circumstances involved.
 - i. understand that their user credentials (user name and password) must not be shared with anyone. End Users will keep their credential information secure. This applies to credentials used to access the site directly or indirectly through a third party application.

Contractor is responsible for oversight and compliance of their End Users. DHHS reserves the right to conduct onsite inspections to monitor compliance with this Contract, including the privacy and security requirements provided in herein, HIPAA, and other applicable laws and Federal regulations until such time the Confidential Data is disposed of in accordance with this Contract.

V. LOSS REPORTING

The Contractor must notify the State's Privacy Officer and Security Officer of any Security Incidents and Breaches immediately, at the email addresses provided in Section VI.

The Contractor must further handle and report Incidents and Breaches involving PHI in

New Hampshire Department of Health and Human Services

Exhibit K

DHHS Information Security Requirements



accordance with the agency's documented Incident Handling and Breach Notification procedures and in accordance with 42 C.F.R. §§ 431.300 - 306. In addition to, and notwithstanding, Contractor's compliance with all applicable obligations and procedures, Contractor's procedures must also address how the Contractor will:

1. Identify Incidents;
2. Determine if personally identifiable information is involved in Incidents;
3. Report suspected or confirmed Incidents as required in this Exhibit or P-37;
4. Identify and convene a core response group to determine the risk level of Incidents and determine risk-based responses to Incidents; and
5. Determine whether Breach notification is required, and, if so, identify appropriate Breach notification methods, timing, source, and contents from among different options, and bear costs associated with the Breach notice as well as any mitigation measures. Incidents and/or Breaches that implicate PI must be addressed and reported, as applicable, in accordance with NH RSA 359-C:20.

VI. PERSONS TO CONTACT

A. DHHS Privacy Officer:

DHHSPrivacyOfficer@dhhs.nh.gov

B. DHHS Security Officer:

DHHSInformationSecurityOffice@dhhs.nh.gov

State of New Hampshire

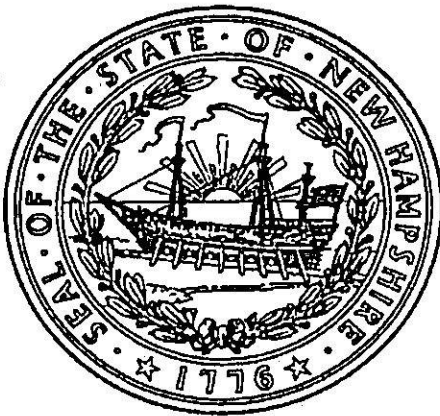
Department of State

CERTIFICATE

I, David M. Scanlan, Secretary of State of the State of New Hampshire, do hereby certify that FIRST DATA GOVERNMENT SOLUTIONS, LIMITED PARTNERSHIP a Delaware Limited Partnership formed to do business in New Hampshire as FDGS, LIMITED PARTNERSHIP on August 17, 2006. I further certify that it has paid the fees required by law and has not dissolved.

Business ID: 563130

Certificate Number: 0005767549



IN TESTIMONY WHEREOF,

I hereto set my hand and cause to be affixed
the Seal of the State of New Hampshire,
this 27th day of April A.D. 2022.

A handwritten signature in black ink, appearing to read "David M. Scanlan".

David M. Scanlan
Secretary of State

CERTIFICATE OF AUTHORITY

I, Jose Garcia, hereby certify that:

1. I am the duly elected President, Secretary, and Treasurer of First Data Government Solutions, LP, a Delaware limited partnership.

2. Shane McCullough is duly authorized on behalf of First Data Government Solutions, LP to enter into contracts or agreements with the State of New Hampshire and any of its agencies or departments and further is authorized to execute any and all documents, agreements and other instruments, and any amendments, revisions, or modifications thereto, which may in his/her judgment be desirable or necessary to effect the purpose of this vote.

3. I hereby certify that Shane McCullough's authority to enter into contracts or agreements on behalf of First Data Government Solutions, LP has not been revoked or repealed and remains in full force and effect as of the date of the contract/contract amendment to which this certificate is attached. This authority **remains valid for thirty (30)** days from the date of this Certificate of Authority. I further certify that it is understood that the State of New Hampshire will rely on this certificate as evidence that the person(s) listed above currently occupy the position(s) indicated and that they have full authority to bind the corporation. To the extent that there are any limits on the authority of any listed individual to bind the corporation in contracts with the State of New Hampshire, all such limitations are expressly stated herein.

Dated: 9/1/2022



Signature of Elected Officer

Name: Jose Garcia

Title: President, Secretary, and Treasurer



CERTIFICATE OF LIABILITY INSURANCE

7/1/2023

DATE (MM/DD/YYYY)

6/28/2022

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

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

PRODUCER Lockton Companies 444 W. 47th Street, Suite 900 Kansas City MO 64112-1906 (816) 960-9000 ketsu@lockton.com	CONTACT NAME: PHONE (A/C, No, Ext): FAX (A/C, No): E-MAIL ADDRESS: <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="text-align: left;">INSURER(S) AFFORDING COVERAGE</th> <th style="text-align: left;">NAIC #</th> </tr> <tr> <td>INSURER A: National Union Fire Ins Co Pitts. PA</td> <td>19445</td> </tr> <tr> <td>INSURER B: *** SEE ATTACHMENT ***</td> <td></td> </tr> <tr> <td>INSURER C: Markel American Insurance Company</td> <td>28932</td> </tr> <tr> <td>INSURER D:</td> <td></td> </tr> <tr> <td>INSURER E:</td> <td></td> </tr> <tr> <td>INSURER F:</td> <td></td> </tr> </table>	INSURER(S) AFFORDING COVERAGE	NAIC #	INSURER A: National Union Fire Ins Co Pitts. PA	19445	INSURER B: *** SEE ATTACHMENT ***		INSURER C: Markel American Insurance Company	28932	INSURER D:		INSURER E:		INSURER F:	
INSURER(S) AFFORDING COVERAGE	NAIC #														
INSURER A: National Union Fire Ins Co Pitts. PA	19445														
INSURER B: *** SEE ATTACHMENT ***															
INSURER C: Markel American Insurance Company	28932														
INSURER D:															
INSURER E:															
INSURER F:															
INSURED 1383155 FISERV INC. IT'S SUBSIDIARIES AND DIVISIONS INCLUDING FIRST DATA GOVERNMENT SOLUTIONS. LP 255 FISERV DRIVE BROOKFIELD WI 53045															

COVERAGES **CERTIFICATE NUMBER:** 18452882 **REVISION NUMBER:** XXXXXXXX

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

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: <input type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input checked="" type="checkbox"/> LOC OTHER:	N	N	1947025	7/1/2022	7/1/2023	EACH OCCURRENCE \$ 1,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 1,000,000 MED EXP (Any one person) \$ 10,000 PERSONAL & ADV INJURY \$ 1,000,000 GENERAL AGGREGATE \$ 2,000,000 PRODUCTS - COMPIOP AGG \$ 2,000,000 \$
A	AUTOMOBILE LIABILITY <input checked="" type="checkbox"/> ANY AUTO <input type="checkbox"/> OWNED AUTOS ONLY <input type="checkbox"/> HIRED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input type="checkbox"/> NON-OWNED AUTOS ONLY	N	N	1722397	7/1/2022	7/1/2023	COMBINED SINGLE LIMIT (Ea accident) \$ 1,000,000 BODILY INJURY (Per person) \$ XXXXXXXX BODILY INJURY (Per accident) \$ XXXXXXXX PROPERTY DAMAGE (Per accident) \$ XXXXXXXX \$ XXXXXXXX
C	<input checked="" type="checkbox"/> UMBRELLA LIAB <input checked="" type="checkbox"/> OCCUR <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE DED <input checked="" type="checkbox"/> RETENTION \$ 10,000	N	N	MKLM6MM70000535	7/1/2022	7/1/2023	EACH OCCURRENCE \$ 5,000,000 AGGREGATE \$ 5,000,000 \$ XXXXXXXX
B	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	Y/N	N/A	SEE ATTACHED	7/1/2022	7/1/2023	<input checked="" type="checkbox"/> PER STATUTE <input type="checkbox"/> OTH-ER E.L. EACH ACCIDENT \$ 1,000,000 E.L. DISEASE - EA EMPLOYEE \$ 1,000,000 E.L. DISEASE - POLICY LIMIT \$ 1,000,000
B	CRIME / E&O / CYBER	N	N	SEE ATTACHED	7/1/2022	7/1/2023	SEE ATTACHED

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

CRIME COVERAGE: CARRIER WILL PAY FOR LOSS OR DAMAGE TO MONEY SECURITIES & OTHER PROPERTY SUSTAINED BY THE NAMED INSUREDS CLIENT RESULTING DIRECTLY FROM THEFT COMMITTED BY AN IDENTIFIED EMPLOYEE ACTING ALONE OR IN COLLUSION WITH OTHER PERSONS. LIMITS \$5,000,000 EACH LOSS, EMPLOYEE DISHONESTY/THEFT.

CERTIFICATE HOLDER
CANCELLATION See Attachment

18452882 State of NH Department of Health and Human Services 129 Pleasant Street Concord NH 03301-3857	SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS. AUTHORIZED REPRESENTATIVE
---	--

© 1988-2015 ACORD CORPORATION. All rights reserved.

Additional Coverage Information

Coverage	Carrier	Policy Number	Limit	Effective Dates ¹
Crime	Zurich American Insurance Company (Zurich)	FID576143109	\$5,000,000 Per Occurrence	7/1/2022 - 7/1/2023
E&O/Cyber	Columbia Casualty Company (CNA)	425578647	\$5,000,000 Per Claim / Aggregate	7/1/2022 - 7/1/2023

Workers Compensation / Employers Liability

Policy Number	States Covered	Issuing Company	Policy Effective Date/Limits
WC 48425935	AOS	AIU INSURANCE CO. (AIG)	7/1/2022 - 7/1/2023 See Acord 25 for applicable limits
WC 48425936	CA	AIU INSURANCE CO. (AIG)	
WC 48425938	WI	AIU INSURANCE CO. (AIG)	
WC 013759690	NY	AIU INSURANCE CO. (AIG)	