DHS Optum

STATE OF MINNESOTA
MNSITE Work Order Contract

This Work Order Contract is between the State of Minnesota, acting through its Department of Human Services ("State") and Optum Government Solutions, doing business as Optum Government Solutions, Inc., 11000 Optum Circle, Eden Prairie, Minnesota 55344 ("Contractor").

Work Order

1. Term of Work Order

1.1. Effective date: The Effective Date of this Work Order Contract is October 24, 2025, or the date the State obtains all required signatures under Minn. Stat. § 16C.05, subd. 2, whichever is later. The Contractor must not begin work under this Work Order Contract until it is fully executed and the Contractor has been notified by the State's Authorized Representative to begin the work.

1.2. Expiration date: The Expiration Date of this Work Order Contract is October 23, 2026, or until all obligations have been satisfactorily fulfilled, whichever occurs first.

1.3. Issuing Authority and Incorporation of Terms: This Work Order Contract is issued under the authority of Master Contract T-Number 23ASK, SWIFT Contract Number 228765, and is subject to all provisions of the Master Contract which is incorporated herein in its entirety, by reference, and is available upon request from the State's Authorized Representative or the Office of State Procurement.

2. Contractor's Duties

2.1. Contractor will perform a Background Check, as detailed in the Master Contract T-Number: 23ASK, on any individual assigned to this Work Order Contract prior to the performance of any work under this agreement.

2.2. The Contractor, who is not a state employee, shall provide state-approved Consultant(s). Consultant(s), who are not state employees, shall perform duties as follows:

2.2.1. Contractor shall assign Consultant(s) to perform the duties specified in Attachment A, which is attached and incorporated in this Work Order Contract.

2.3. Contractor will provide weekly status or progress updates to the State project manager or team leads.

3. Consideration and Payment

3.1. Consideration. The State will pay for all services performed by the Contractor under this Work Order Contract as follows:

3.1.1. Compensation. The Contractor will be paid as follows: An hourly rate of $177.00 for any resource placed under this agreement.

3.1.2. Total Obligation. The total obligation of the State for all compensation and reimbursements to the Contractor under this Work Order Contract will not exceed $2,315,160.00 USD.

3.2. Invoices. The State will promptly pay the Contractor after the Contractor presents an itemized invoice for the services actually performed and the State's Authorized Representative accepts the invoiced services. Invoices must be submitted timely and according to the following schedule: On a monthly basis following the preceding month in which services have been delivered. Invoices must include a breakdown of hours for each resource for the month and show a completion percentage for each of the Phases identified in Attachment A for the given month. Invoices must be sent via email to the State Authorized Representative listed below in Clause 5. All Invoices must include the SWIFT Contract ID Number and Purchase Order Number, which are found on the Signature page under Signature Block 1.

4. State Assumptions:

4.1. Claims adjustment, processing and approval role is with DHS State Staff.

4.2. State Onboarding process will be efficient.

5. Work Order Authorized Representative and Project Managers

The State's Authorized Representative/Project Manager is:

The State's Work Order Authorized Representative (or his/her successor) has the authority to accept the services provided under this Work Order. If the services are satisfactory, the State's Authorized Representative will certify acceptance on each invoice submitted for payment. The State's Authorized Representative is:
Name: George McNulty
Title: CBTO
Email: george.mcnulty@state.mn.us

The State's Work Order Project Manager (or his/her successor) has the responsibility to monitor the Contractor's performance. The State's Project Manager is:
Name: Dan DeZiel
Title: Project Manager
Email: dan.deziel@state.mn.us

The Contractor's Project Manager is:
Name: Kevin Hutchinson
Title: VP, Business Development
Email: kevin.hutchinson@optum.com
Phone: 763-330-7785
If the Contractor's Project Manager changes at any time during this work order, the Contractor must immediately notify the State.

6. Liability/Indemnification

The Contractor must indemnify, save, and hold State, its agents, and employees harmless from any claims or causes of action, including reasonable attorney's fees incurred by the State for damages directly and proximately caused by the negligence of the Contractor while engaged in the performance of services under this contract. As a condition to the foregoing indemnity obligations, State shall provide the Contractor with prompt notice of any claim for which indemnification shall be sought hereunder and shall cooperate in all reasonable respects with the Contractor in connection with any such claim. In accordance with Minnesota Statutes, Section 8.06, for claims against the State, the State's Attorney General's Office must provide consent and approval with respect to Contractor's ability and right to control the handling of any such claim and to defend or settle any such claim with counsel of its own choosing.

The Contractor, its principals, members and employees shall not be liable to State for any actions, damages, claims, liabilities, costs, expenses, or losses in any way arising out of or relating to the services performed hereunder for an aggregate amount excess of two (2) times the Work Order Contract amount or $2,000,000, whichever is greater. In no event shall Contractor, its principals, members, or employees be liable for consequential, special, indirect, incidental, punitive, or exemplary damages, costs, expenses, or losses (including, without limitation, lost profits and opportunity costs).

7. Diverse Spend Reporting

If the total value of the Work Order Contract may exceed $500,000, including all extension options, Contractor must track and report, on a quarterly basis, the amount paid to diverse businesses both: 1) directly to subcontractors performing under the Work Order Contract, and 2) indirectly to diverse businesses that provide supplies/services to your company (in proportion to the revenue from this Work Order Contract compared to Contractor's overall revenue). When this applies, Contractor will register in a free portal to help report the Tier 2 diverse spend, and the requirement continues as long as the Work Order Contract is in effect.

8. Information Privacy and Security.

Information privacy and security will be governed by the "Data Sharing and Business Associate Agreement Terms and Conditions," which is attached and incorporated into this Work Order Contract as Attachment B.

8.1. Contractor's work must comply with the State of Minnesota's Enterprise Information Security Policy and Standards.

8.2. The Contractor must supply a mutually agreeable security audit on the CES Assessment as well as the Pre-Pay Environment (pre-pay solution created by Contractor pursuant to Attachment A) prior to State-owned data being ingested into these environments.

8.3. Contractor may only process and store State-owned data in data centers that are located in the forty-eight (48) contiguous United States.

8.4. The Contractor must ensure that all State-owned data is encrypted in transit and at rest per MN data encryption level.

8.5. State must maintain sole legal ownership of State-owned data as it exists in the payment integrity solution.

8.6. Contractor must comply with Minnesota statutes per Chapter 13 Government Data Practices.

8.7. Contractor must conform to the Guidelines for record retention in DHS Licensed Programs, as applicable.

1. STATE ENCUMBRANCE VERIFICATION
*Individual certifies that funds have been encumbered as required by Minn. Stat. §§*16A.15 and 16C.05.

Signed: DocuSigned by: Angela Lofgren 53AD6200B0B8428...

Date: 10/23/2025

SWIFT Contract ID: 277977 PO# 3000121850

2. Optum Government Solutions (CONTRACTOR)
The Contractor certifies that the appropriate person(s) have executed the contract on behalf of the Contractor as required by applicable articles or bylaws.

By: Signed by: Diane M Evenson 858CA32936DE4F9...

Title: VP, Regional General Manager

Date: 10/23/2025

3. Department of Human Services (STATE AGENCY)

By: DocuSigned by: Jeffrey Jorgenson D701E4038E794C5...
(with delegated authority)

Title: Business Transformation Officer

Date: 10/23/2025

4. COMMISSIONER OF ADMINISTRATION
As delegated to the Office of State Procurement

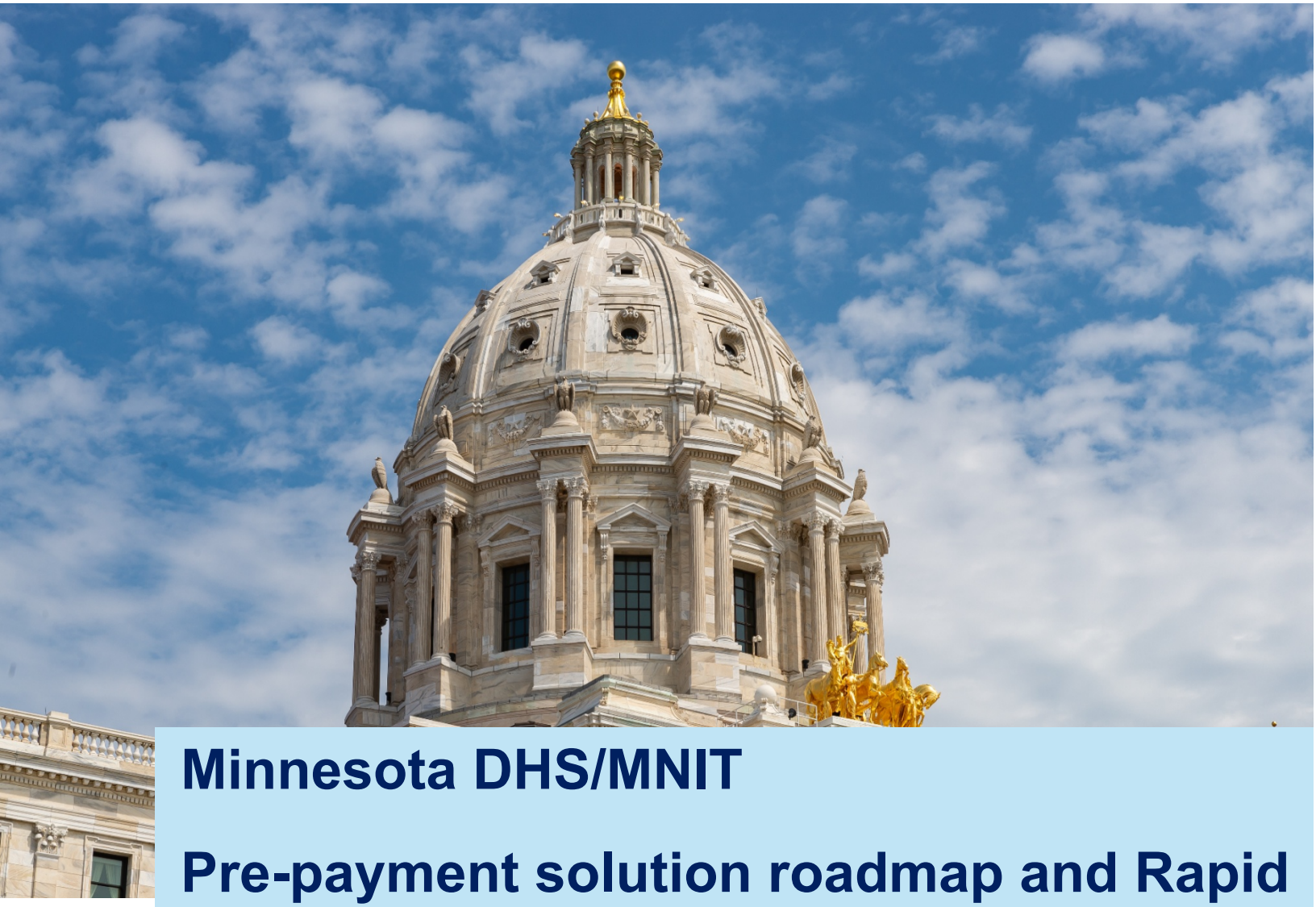
By: DocuSigned by: Mark Haselman 27F2E3577E6D4CB...

Date: 10/23/2025

TBD

Optum

ATTACHMENT A



Minnesota DHS/MNIT

Pre-payment solution roadmap and Rapid Response Team to improve detection of Fraud, Waste and Abuse in DHS health care programs

Updated October 21, 2025

Plan and Statement of Work

Fraud Package DDI And M&O
Vendor Part #: OSGS48001
SIN: 54151ECOM

Contact
Kevin Hutchinson
VP, Client Relationship Executive
Optum
P: 763-330-7785
E: kevin.hutchinson@optum.com

One Year Roadmap for Improved Payment Integrity and Fraud, Waste and Abuse Detection and Interdiction Prior to Payment Processing

Optum is pleased to present the Minnesota Department of Human Services (DHS) and the Minnesota Department of IT (MNIT) with a Two-Phase Plan Statement of Work (SOW) for establishing an AI-enabled pre-payment program integrity initiative. This one-year effort, based on initial evaluations, will lay the foundation for future deployment of a Claims Editing System and Pre-pay Review Solution tailored to Minnesota's distinctive policies, programs, and Medicaid Managed Care Organization environment. This approach will identify the areas of vulnerabilities in the claims process, flag potential FWA prior to payment, and operationalize the pre-pay approach to complement the post-pay FWA already in place within MNIT, DHS and the DHS OIG.

Phase 1: Rapid Response Team (RRT), Pre-pay Review and Claims Editing

Timeline: First 90 days after contract execution.

The primary objective of this phase is to conduct a comprehensive evaluation of fraud, waste, and abuse (FWA) across 13 high-risk service/programs (listed below). This includes quantifying MMIS claim edits, identifying cost avoidance and recovery opportunities, and launching pre-payment strategies to improve long-term savings and operational efficiency.

Expected outcomes include:

- Clear identification of FWA patterns and vulnerabilities
- Measurable estimates of cost avoidance and recoveries
- Strategic recommendations for pre-payment prevention and process improvements
- Set up of the hybrid pre-prepayment solution

Priority	High Risk Service/Program Name
1	Peer Recovery
2	Early Intensive Developmental and Behavioral Intervention (EIDBI)
3	Non-Emergency Medical Transportation (NEMT)
4	Adult Rehabilitative Mental Health Services (ARMHS)
5	Personal Care Assistance (PCA) / Community First Services and Supports (CFSS)
6	Home and Community Based Service - Integrated Community Supports (HCBS-ICS)
7	Adult Day Center
8	Recuperative Care
9	Individualized Home Supports (without training, with training, with family training)
10	Companion Care
11	Night Supervision
12	Assertive Community Treatment (ACT)
13	Intensive Residential Treatment Service (IRTS)

Scope of Work:

- Optum RRT will accelerate and augment FWA data analytic development.
    - We will deploy AI Policy to SQL Engine to assist in algorithm development and review of the State's identified 13 high-risk service/programs.
    - We will conduct an initial assessment of the current list of Program Integrity Oversight Division (PIOD) algorithms to determine gaps.
    - We will leverage the Teradata Enterprise Data Warehouse (EDW) to:
        - identify and report potential FWA,
        - opportunities for new MMIS edits/claims accuracy,
        - opportunities for prepay FWA detection.
    - We will deliver actionable results to include a summary / overview background (supporting policy), methodology, findings and recommendations to DHS, MNIT and OIG. Depending on the findings, recommendations may address key areas of vulnerability, outline financial exposure, and present projected cost avoidance, offering actionable insights to support informed decision-making and resource optimization.
- Prepare and deliver a summary report outlining key achievements, cost savings trends, and any findings or recommendations. The report is due by December 26, 2025. This report may represent the current status of the initiative with (a) subsequent report(s) to be delivered at a later date.
- Optum will begin implementation the Prepayment FWA Solution using the developed algorithms into the MMIS claims stream, deploying a hybrid approach.
- The "hybrid" prepayment solution is defined as follows:
    - Using data from existing data sources, rather than a purpose-built data feed, and using the data in its existing format(s).
    - Running analytics (custom-developed SQL queries) in State systems vs. in the Optum pre-pay system.
    - Running analytics at a lower frequency (every two weeks vs. daily), and with a longer turn-around time, likely to be required with minimal implementation/setup time.
    - Conducting some degree of manual review of analytic findings as a quality check before sending the file to the State/MMIS. This is likely be more necessary in the first 30 – 60 days of pre-pay operations. This function is performed by the Optum FWA Prepayment team.
    - Providing a prepayment report and/or suspend claims file which the State MMIS team will need to work to integrate into the MMIS workflow to successfully suspend the suspect claims. This will occur in each warrant cycle with reports provided to the State with enough time provided for the state take action.
- Establish the hybrid prepayment claims-analysis solution as defined above which is executed on MN infrastructure no later than November 30, 2025.

- Optum will support this by leveraging existing steps in the MMIS claims flow, deploying additional staff to handle the necessary claims processing, working with DHS to fully operationalize the workflow, and identifying reporting needed to support the establishment of a new DHS workflow and federal reporting. This work includes the following:
    - Flag claims according to initial vendor criteria for FWA (distilled from RRT-developed algorithms)
    - Engage DHS SMEs to check assumptions (e.g., are these claims improper?)
    - Assume this process is iterative and that learnings will occur on all sides
    - Refine data analysis approach based on learnings
    - Adjust claims to be paid, denied, or to remain in suspense (pending further review) based on investigation results
    - Interface with DHS technology to communicate back to providers if additional data or documentation is required to adjudicate claims in question
    - Flag high-risk claims weekly before release for payment and determine workflow.
    - Facilitate provider impact monitoring to reduce abrasion.
- Optum will conduct a Claims Editing System Assessment to pinpoint vulnerabilities in claims editing and policy enforcement, identify opportunities for improvement, and identify preliminary ROI.

Optum Resources

- Optum will assign a full-time project manager with oversight provided by an account manager.
- The RRT will include four (4) program integrity data analyst responsible for identifying and evaluating potential fraud, waste, and abuse patterns, along with a data engineer who will assist with advanced query development and data management.
- The FWA Prepayment team will consist of a Fraud, Waste, and Abuse Solutions Specialist and a Claims Processing Analyst, combining strategic expertise with operational insight to support prepayment integrity efforts.

Phase 2: Rapid Response Team (RRT), and Pre-pay Review

Timeline: Month four (4) through month twelve (12)

The objective is to continuously advance data mining and algorithmic capabilities to enhance visibility into the scale and complexity of Fraud, Waste, and Abuse (FWA) across in scope Medicaid programs. This includes:

- **Refining the operationalization** of a hybrid solution to prevent improper payments within the MMIS claims stream.
- **Continuing implementation** of the Prepay FWA Solution launch.

Scope of Work:

- Optum RRT will continue to accelerate and augment FWA data analytic development and expand the review to additional in-scope Medicaid programs.
    - Optum's RRT will leverage the Teradata Enterprise Data Warehouse (EDW) to:
        - Identify and report potential FWA,
        - opportunities for new MMIS edits/claims accuracy,
        - opportunities for prepay FWA detection.
    - We will deliver actionable results to include a summary / overview background (supporting policy), methodology, findings and recommendations to DHS, MNIT and OIG. Depending on the findings, recommendations may address key areas of vulnerability, outline financial exposure, and present projected cost avoidance, offering actionable insights to support informed decision-making and resource optimization.
- Optum will continue operations of the Prepayment FWA Solution using the developed algorithms into the MMIS claims stream. Optum will support this by leveraging existing steps in the MMIS claims flow, deploying additional staff to handle the necessary claims processing, working with DHS to fully operationalize the workflow, and identifying reporting needed to support the establishment of a new DHS workflow and federal reporting. This work includes the following:
    - Flag claims according to initial vendor criteria for FWA (distilled from RRT-developed algorithms)
    - Engage DHS SMEs to check assumptions (e.g., are these claims improper?)
    - Assume this process is iterative and that learnings will occur on all sides
    - Refine data analysis approach based on learnings
    - Adjust claims to be paid, denied, or to remain in suspense (pending further review) based on investigation results
    - Interface with DHS technology to communicate back to providers if additional data or documentation is required to adjudicate claims in question

- Flag high-risk claims weekly before release for payment and determine workflow.
- Facilitate provider impact monitoring to reduce abrasion.

Optum Resources

- Resources will be continued from Phase I
  - A full-time project manager with oversight provided by an account manager.
  - The RRT will include four (4) program integrity data analyst responsible for identifying and evaluating potential fraud, waste, and abuse patterns, along with a data engineer who will assist with advanced query development and data management.
  - The FWA Prepayment team will consist of a Fraud, Waste, and Abuse Solutions Specialist and a Claims Processing Analyst, combining strategic expertise with operational insight to support prepayment integrity efforts.

Optum Phase 1 & 2 Assumptions

ID	Phase	Area	Assumptions & Dependencies
1	1	Project Management	Minnesota DHS Medicaid policy (Provider Manual) is accessible online and maintained with current updates to ensure alignment with state and federal regulations.
2	1	Project Management	Minnesota DHS / MNIT will provide Optum with a list with detailed descriptions of the current MMIS claim edits.
3	1	Project Management	Program Integrity Oversight Division (PIOD) will provide a list of the current algorithms to be used in initial assessment of gaps.
4	1	Technology	Minnesota DHS / MNIT will provide the Optum staff with secure workstations on the MN network. These workstations will have the appropriate software installed with access for eight users (8) to the data warehouse no later than five (5) business days after Onboarding Processes complete. This will include basic permissions (select, insert, update) for seven (7) users and then advanced permissions (select, insert, update, delete, execute, create, drop and alter) for the one (1) data engineer. DHS / MNIT will provide Optum users with DHS / MNIT laptops if Optum laptops cannot be configured to connect to the Teradata system.
5	1	Technology	Minnesota DHS / MNIT will provide Optum access to the data warehouse within one week (5 business days) of Onboarding Processes complete.
6	1	Technology	Minnesota DHS / MNIT will provide Optum with the data warehouse DDL and data dictionary, including valid value descriptions, no later than five (5) days after Onboarding Processes complete.
7	1	Technology	Minnesota DHS / MNIT will provide Optum with Microsoft Excel and Word for analysis and delivery of the results.
8	1	Project Management	Optum will have sufficient access to Minnesota DHS/ MNIT / PIOD business resources as necessary to aid with SQL logic for identification of the original/final paid claims, as well as any data anomalies.
9	1	Project Management	Optum RRT staffing assumes 6 full-time roles: Project Manager, Sr Data Engineer, Sr Business Analyst and three (3) Sr Data Analyst. A part-time account manager will also be assigned to oversee the project. For Prepay FWA Solution, a half-time Claims Processor and a half-time Claims Fraud SME will also support the project starting in the second month of Phase 1.
10	1	Reporting	Optum will provide an Executive Summary along with detailed, actionable insights delivered in Excel format for all pre-approved algorithms.
11	1	Project Management	Minnesota DHS / MNIT will provide Optum with office space and meeting room(s) sufficient for the Optum team when the team is onsite with DHS/MNIT.
12	1	Claims Editing System	Minnesota DHS/MNIT will provide Optum 3-12 months of paid claims data based on attachment XX - Data Submission Guide_CES_Product Assessments 2025.xlsx or a mutually agreed format.

		Assess ment	
13	2	Project Manage ment	Given the anticipated change in the claims process, we assume that the State will be prepared for a significant increase in pended claims.
14	2	Project Manage ment	Optum is assuming for the prepay FWA component that the State will be doing the investigations. Optum has the capacity to take on this work, but State will decide at a later date how they would like to manage this portion and an addendum, if needed, will be written to accommodate the decision.

Software and Configuration Required for Optum Personnel on MN workstations.

Purpose	Software Application	Target User/Role	Notes
Run classic SQL queries	Teradata SQL Assistant	Business Analyst	Lightweight query tool
Develop and manage SQL workflows	Teradata Studio	Data Engineer	Full-featured SQL IDE
Productivity and documentation	Microsoft Office Suite	All Roles	Includes Excel, Word, PowerPoint, Outlook
Clipboard and file access in virtual desktops	VMware Horizon Client / Citrix / Azure VDI	All VDI Users	Clipboard redirection enabled
File sharing and communication	Email/OneDrive/SharePoint/S FTP	All VDI Users	Secure file transfer and collaboration

Pricing for Phase 1 & Phase 2

Phase / Role	Hours	Amount
Rapid Response Team		
Account Manager	120	$21,240
FWA B/A Lead	1,920	$339,840
FWA Data Analyst	1,920	$339,840
FWA Data Analyst	1,920	$339,840
FWA Data Analyst	1,920	$339,840
FWA Data Engineer	1,920	$339,840
PM	1,920	$339,840
Total Rapid Response Team	**11,640**	**$2,060,280**
Pre-Pay FWA		
Claims Processor	720	$127,440
FWA SME	720	$127,440
Total Pre-Pay FWA	**1,440**	**$254,880**
Total	**13,080**	**$2,315,160**

Pricing Notes:

- Hours are charged at $177.00 per hour

ATTACHMENT B
DATA SHARING AND BUSINESS ASSOCIATE AGREEMENT
TERMS AND CONDITIONS

This Attachment sets forth the terms and conditions in which STATE will share data with and permit Optum Government Solutions, Inc. ("CONTRACTOR") to use or disclose Protected Information that the parties are legally required to safeguard pursuant to the Minnesota Data Practices Act under Minnesota Statutes, chapter 13, the Health Insurance Portability and Accountability Act rules and regulations codified at 45 C.F.R. Parts 160, 162, and 164 ("HIPAA") and other applicable laws.

The parties agree to comply with all applicable provisions of the Minnesota Data Practices Act, HIPAA, and any other state and federal statutes that apply to the Protected Information.

Under the contract associated with this data sharing and business associate's agreement ("BAA"), the services will provide the foundation for future deployment of a Claims Editing System and Pre-pay Review Solution tailored to Minnesota's distinctive policies, programs, and Medicaid Managed Care Organization environment. This approach will identify the areas of vulnerabilities in the claims process, flag potential fraud, waste, and abuse (FWA) prior to payment, and operationalize the pre-pay approach to complement the post-pay FWA already in place within MNIT, DHS and the DHS Office of Inspector General (OIG).

Purpose for Sharing Protected Information and Expected Outcomes: In order to allow CONTRACTOR to conduct an AI-enabled pre-payment program integrity initiative pursuant to Minnesota's Executive Order 25-10.

In addition, STATE will provide CONTRACTOR with access to STATE's MMIS claims data and Enterprise Data Warehouse claims data in order for CONTRACTOR to conduct its fraud, waste and abuse assessment of the system. As a result, CONTRACTOR may have access to the information stored in the system, which includes not-public information about individual participants and providers in STATE programs, including individuals' names, addresses, contact information, income, and medical information (which includes medical diagnoses and program eligibility status). This information includes protected health information, and other information designated by State law as not-public data.

STATE is permitted to share the Protected Information with CONTRACTOR pursuant to Minnesota Statutes, section 13.46, subds. 2(a)(4) and (6), 45 C.F.R. 164.506, Chapter 16E (and in particular Minn. Stat. 16E.01, subsection 1a, under which the STATE's Office of MN.IT Services is authorized to protect the security of information technology systems).

It is expressly agreed that CONTRACTOR is a "business associate" of STATE, as defined by HIPAA under 45 C.F.R. § 160.103. The disclosure of protected health information to GRANTEE that is subject to the Health Insurance Portability Accountability Act (HIPAA) is permitted by 45 C.F.R. § 164.502(e)(1)(i).

DEFINITIONS

A. "Agent" means CONTRACTOR'S employees, contractors, subcontractors, and other non-employees and representatives.

B. “Applicable Safeguards” means the state and federal provisions listed in Section 2.1 of this Attachment.

C. “Breach” means the acquisition, access, use, or disclosure of unsecured protected health information in a manner not permitted by HIPAA, which compromises the security or privacy of protected health information.

D. “Business associate” shall generally have the same meaning as the term “business associate” at 45 C.F.R. § 160.103, and in reference to the party in the Contract and this Attachment, shall mean CONTRACTOR.

E. “Contract” means the Professional/Technical Contract between STATE and CONTRACTOR.

F. “Disclosure” means the release, transfer, provision of access to, or divulging in any manner of information by the entity in possession of the Protected Information.

G. “HIPAA” means the rules and regulations codified at 45 C.F.R. Parts 160, 162, and 164.

H. “Individual” means the person who is the subject of protected information.

I. “Privacy incident” means a violation of an information privacy provision of any applicable state and federal law, statute, regulation, rule, or standard, including those listed in the Contract and this Attachment.

J. “Protected information” means any information that is or will be used by STATE or CONTRACTOR under the Contract that is protected by federal or state privacy laws, statutes, regulations or standards, including those listed in this Attachment. This includes, but is not limited to, individually identifiable information about a State, county or tribal human services agency client or a client’s family member. Protected information also includes, but is not limited to, protected health information, as defined below, and protected information maintained within or accessed via a State information management system, including a State “legacy system” and other State application.

K. “Protected health information” is a subset of “individually identifiable health information” in accordance with 45 C.F.R. § 160.103, but for purposes of this Attachment refers only to that information that is received, created, maintained, or transmitted by CONTRACTOR as a business associate on behalf of DHS. Protected health information is a specific subset of protected information as defined above.

L. “Security incident” means the attempted or successful unauthorized use or the interference with system operations in an information management system or application. Security incident does not include pings and other broadcast attacks on a system’s firewall, port scans, unsuccessful log-on attempts, denials of service, and any combination of the above, provided that such activities do not result in the unauthorized use of Protected Information.

M. "Use" or "used" means any activity by the parties during the duration of the Contract involving protected information including its creation, collection, access, use, modification, employment, application, utilization, examination, analysis, manipulation, maintenance, dissemination, sharing, disclosure, transmission, or destruction. Use includes any of these activities whether conducted manually or by electronic or computerized means.

N. "User" means an agent of either party, who has been authorized to use protected information.

1. INFORMATION EXCHANGED

1.1 This Attachment governs the data that will be exchanged pursuant to CONTRACTOR performing the services described in the Contract. The data exchanged under the Contract will include not-public data on individual participants and providers (names, addresses, contact information, income, medical diagnoses, program eligibility status, and other medical information). This information includes protected health information, and other information designated by State law as not-public data.

1.2 The data exchanged under the Contract is provided to CONTRACTOR in order for CONTRACTOR to provide the foundation for future deployment of a Claims Editing System and Pre-pay Review Solution tailored to Minnesota's distinctive policies, programs, and Medicaid Managed Care Organization environment. This approach will identify the areas of vulnerabilities in the claims process, flag potential FWA prior to payment, and operationalize the pre-pay approach to complement the post-pay FWA already in place within MNIT, DHS and the DHS OIG.

1.3 STATE is permitted to share the Protected Information with CONTRACTOR pursuant to Minnesota Statutes, section 13.46, subds. 2(a)(4) and (6), 45 C.F.R. 164.506, and Chapter 16E (in particular Minn. Stat. 16E.01, subsection 1a).

2. INFORMATION PRIVACY AND SECURITY

CONTRACTOR and STATE must comply with the Minnesota Government Data Practices Act, Minn. Stat. § 13, and the Health Insurance Portability Accountability Act ["HIPAA"], 45 C.F.R. § 164.103, et seq., as it applies to all data provided by STATE under the Contract, and as it applies to all data created, collected, received, stored, used, maintained, or disseminated by CONTRACTOR under the Contract. The civil remedies of Minn. Stat. § 13.08 apply to CONTRACTOR and STATE. Additionally, the remedies of HIPAA apply to the release of data governed by that Act.

2.1 Compliance with Applicable Safeguards.

A. State and Federal Safeguards. The parties acknowledge that the Protected Information to be shared under the terms of the Contract may be subject to one of the following laws, statutes, regulations, rules, and standards, as applicable ("Applicable Safeguards"). The parties agree to comply with all rules, regulations and laws, including as amended or revised, applicable to the exchange, use and disclosure of data under the Contract.

1. Health Insurance Portability and Accountability Act rules and regulations codified at 45 C.F.R. Parts 160, 162, and 164 ("HIPAA");
2. Minnesota Government Data Practices Act (Minn. Stat. Chapter 13);

3. Minnesota Health Records Act (Minn. Stat. §144.291 - 144.298);
4. Confidentiality of Alcohol and Drug Abuse Patient Records (42 U.S.C. § 290dd-2 and 42 C.F.R. § 2.1 to §2.67);
5. Tax Information Security Guidelines for Federal, State and Local Agencies (26 U.S.C. 6103 and Publication 1075);
6. U.S. Privacy Act of 1974;
7. Computer Matching Requirements (5 U.S.C. 552a);
8. Social Security Data Disclosure (section 1106 of the Social Security Act);
9. Disclosure of Information to Federal, State and Local Agencies (DIFSLA Handbook" Publication 3373);
10. Final Exchange Privacy Rule of the Affordable Care Act (45 C.F.R. § 155.260); and
11. NIST Special Publication 800-53, Revision 4 (NIST.SP.800-53r4).

B. Statutory Amendments and Other Changes to Applicable Safeguards. The Parties agree to take such action as is necessary to amend the Contract and this Attachment from time to time as is necessary to ensure, current, ongoing compliance with the requirements of the laws listed in this Section or in any other applicable law.

2.2 CONTRACTOR Data Responsibilities

A. Use Limitation.

1. Restrictions on Use and Disclosure of Protected Information. Except as otherwise authorized in the Contract or this Attachment, CONTRACTOR may only use or disclose Protected Information as necessary to provide the services to STATE as described herein, or as otherwise required by law, provided that such use or disclosure of Protected Information, if performed by STATE, would not violate the Contract, this Attachment, HIPAA, or other state and federal statutes or regulations that apply to the Protected Information.

2. Federal tax information. To the extent that Protected Information used under the Contract constitutes "federal tax information" (FTI), CONTRACTOR shall ensure that this data only be used as authorized under the Patient Protection and Affordable Care Act, the Internal Revenue Code, 26 U.S.C. § 6103(C), and IRS Publication I075.

B. Individual Privacy Rights. CONTRACTOR shall ensure individuals are able to exercise their privacy rights regarding Protected Information, including but not limited to the following:

1. Complaints. CONTRACTOR shall work cooperatively with STATE to resolve complaints received from an individual; from an authorized representative; or from a state, federal, or other health oversight agency.

2. **Amendments to Protected Information Requested by Data Subject Generally.** Within ten (10) business days, CONTRACTOR must forward to STATE any request to make any amendment(s) to Protected Information in order for STATE to satisfy its obligations under Minn. Stat. § 13.04, subd. 4. If the request to amend Protected Information pertains to Protected Health Information, then CONTRACTOR must also make any amendment(s) to protected health information as directed or agreed to by STATE pursuant to 45 C.F.R. § 164.526 or otherwise act as necessary to satisfy STATE or CONTRACTOR's obligations under 45 CF.R. § 164.526 (including, as applicable, protected health information in a designated record set).

C. Background Review and Reasonable Assurances Required of Agents.

1. **Criminal Background Check Required.** CONTRACTOR and employees of CONTRACTOR accessing STATE's Protected Information must submit to STATE or provide evidence of a computerized criminal history system background check (hereinafter "CCH background check") performed within the last 12 months before work can begin under the Contract. "CCH background check" is defined as a background check including search of the computerized criminal history system of the Minnesota Department of Public Safety's Bureau of Criminal Apprehension.

2. **Reasonable Assurances.** CONTRACTOR represents that, before its Agents are allowed to use or disclose Protected Information, CONTRACTOR has conducted and documented a background review of such Agents sufficient to provide CONTRACTOR with reasonable assurances that the Agent will comply with the terms of the Contract, this Attachment and Applicable Safeguards.

3. **Documentation.** CONTRACTOR shall make available documentation required by this Section upon request by STATE.

D. Ongoing Responsibilities to Safeguard Protected Information.

1. **Privacy and Security Policies.** CONTRACTOR shall develop, maintain, and enforce policies, procedures, and administrative, technical, and physical safeguards to ensure the privacy and security of the Protected Information.

2 **Electronic Protected Information.** CONTRACTOR shall implement and maintain appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 (HIPAA Security Rule) with respect to electronic Protected Information, including electronic Protected Health Information, to prevent the use or disclosure other than as provided for by the Contract or this Attachment.

3. **Monitoring Agents.** CONTRACTOR shall ensure that any contractor, subcontractor, or other agent to whom CONTRACTOR discloses Protected Information on behalf of STATE, or whom CONTRACTOR employs or retains to create, receive, use, store, disclose, or transmit Protected Information on behalf of STATE, agrees to the same restrictions and conditions that apply to CONTRACTOR under the Contract and this Attachment with respect to such Protected Information, and in accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2).

4. **Minimum Necessary Access to Protected Information.** CONTRACTOR shall ensure that its Agents use only the minimum necessary Protected Information needed to complete an authorized and legally permitted activity.

5. **Training.** CONTRACTOR shall ensure that Agents are properly trained and comply with all Applicable Safeguards and the terms of the Contract and this Attachment.

E. Responding to Privacy Incidents, Security Incidents, and Breaches. CONTRACTOR will comply with this Section for all protected information shared under the Contract. Additional obligations for specific kinds of protected information shared under the Contract are addressed in Section 2.2(F).

1. **Mitigation of harmful effects.** Upon discovery of any actual or suspected privacy incident, security incident, or breach, CONTRACTOR will mitigate, to the extent practicable, any harmful effect of the privacy incident, security incident, or breach. Mitigation may include, but is not limited to, notifying and providing credit monitoring to affected individuals.

2. **Investigation.** Upon discovery of any actual or suspected privacy incident, security incident, or breach, CONTRACTOR will investigate to (1) determine the root cause of the incident, (2) identify individuals affected, (3) determine the specific protected information impacted, and (4) comply with notification and reporting provisions of the Contract, this Attachment and applicable law.

3. **Corrective action.** Upon identifying the root cause of any privacy incident, security incident, or breach, CONTRACTOR will take corrective action to prevent, or reduce to the extent practicable, any possibility of recurrence. Corrective action may include, but is not limited to, patching information system security vulnerabilities, employee sanctions, or revising policies and procedures.

4. **Notification to individuals and others; costs incurred.**

   a. **Protected Information.** CONTRACTOR will determine whether notice to data subjects and/or any other external parties regarding any privacy incident or security incident is required by law. If such notice is required, CONTRACTOR will comply with STATE's and CONTRACTOR's obligations under any applicable law requiring notification, including, but not limited to, Minn. Stat. §§ 13.05 and 13.055.

b. **Protected Health Information.** If a privacy incident or security incident results in a breach of protected health information, as these terms are defined in this Attachment, then CONTRACTOR will provide notice to individual data subjects under any applicable law requiring notification, including but not limited to providing notice as outlined in 45 C.F.R. § 164.404.

c. **Failure to notify.** If CONTRACTOR fails to notify individual data subjects or other external parties under subparagraphs (a) and (b), then CONTRACTOR will reimburse STATE for any costs incurred as a result of CONTRACTOR's failure to provide notification.

5. **Obligation to report to STATE.** Upon discovery of a privacy incident, security incident, or breach, CONTRACTOR will report to STATE in writing as specified in Section 2.2(F).

a. **Communication with authorized representative.** CONTRACTOR will send any written reports to, and communicate and coordinate as necessary with, STATE's authorized representative.

b. **Cooperation of response.** CONTRACTOR will cooperate with requests and instructions received from STATE regarding activities related to investigation, containment, mitigation, and eradication of conditions that led to, or resulted from, the security incident, privacy incident, or breach.

c. **Information to respond to inquiries about an investigation.** CONTRACTOR will, as soon as possible, but not later than forty-eight (48) hours after a request from STATE, provide STATE with any reports or information requested by STATE related to an investigation of a security incident, privacy incident, or breach.

6. **Documentation.** CONTRACTOR will document actions taken under paragraphs 1 through 5 of this Section, and provide such documentation to STATE upon request.

F. **Reporting Privacy Incidents, Security Incidents, and Breaches.** CONTRACTOR will comply with the reporting obligations of this Section as they apply to the kind of protected information involved. CONTRACTOR will also comply with Section 2.2(E) above in responding to any privacy incident, security incident, or breach.

1. **Protected Health Information.** CONTRACTOR will report breaches and security incidents involving protected health information to STATE and other external parties. CONTRACTOR will notify STATE, in writing, of (1) any breach or suspected breach of protected health information; (2) any security incident; or (3) any violation of an individual's privacy rights as they involve protected health information created, received, maintained, or transmitted by CONTRACTOR or its Agents on behalf of STATE.

a. **Breach reporting.** CONTRACTOR will report, in writing, any breach of protected health information to STATE within five (5) business days of discovery, in accordance with 45 C.F.R § 164.410.

Content of report to STATE. Reports to the authorized representative regarding breaches of protected health information will include:

1. Identities of the individuals whose unsecured Protected Health Information has been breached.
2. Date of the breach and date of its discovery.
3. Description of the steps taken to investigate the breach, mitigate its effects, and prevent future breaches.
4. Sanctions imposed on members of CONTRACTOR's workforce involved in the breach.
5. Other available information that is required to be included in notification to the individual under 45 C.F.R. § 164.404(c).
6. Statement that CONTRACTOR has notified, or will notify, affected data subjects in accordance with 45 C.F.R. § 164.404.

b. **Security incidents resulting in a breach.** CONTRACTOR will report, in writing, any security incident that results in a breach, or suspected breach, of protected health information to STATE within five (5) business days of discovery, in accordance with 45 C.F.R § 164.314 and 45 C.F.R § 164.410.

c. **Security incidents that do not result in a breach.** CONTRACTOR will report all security incidents that do not result in a breach, but involve systems maintaining protected health Information created, received, maintained, or transmitted by CONTRACTOR or its Agents on behalf of STATE, to STATE on a monthly basis, in accordance with 45 C.F.R § 164.314.

d. **Other violations.** CONTRACTOR will report any other violation of an individual's privacy rights as it pertains to protected health information to STATE within five (5) business days of discovery. This includes, but is not limited to, violations of HIPAA data access or complaint provisions.

e. **Reporting to other external parties.** CONTRACTOR will report all breaches of protected health information to the federal Department of Health and Human Services, as specified under 45 C.F.R 164.408. If a breach of protected health information involves 500 or more individuals:

1. CONTRACTOR will immediately notify STATE.
2. CONTRACTOR will report to the news media and federal Department of Health and Human Services in accordance with 45 C.F.R. §§ 164.406-408.

2. **Other Protected Information.** CONTRACTOR will report all other privacy incidents and security incidents to STATE.

a. **Initial report.** CONTRACTOR will report all other privacy and security incidents to STATE, in writing, within five (5) days of discovery. If CONTRACTOR is unable to complete its investigation of, and response to, a

privacy incident or security incident within five (5) days of discovery, then CONTRACTOR will provide STATE with all information under Section 2.2(E)(1)-(4), of this Attachment that are available to CONTRACTOR at the time of the initial report.

b. Final report. CONTRACTOR will, upon completion of its investigation of and response to a privacy incident or security incident, or upon STATE's request in accordance with Section 2.2(E)(5) submit in writing a report to STATE documenting all actions taken under Section 2.2(E)(1)-(4), of this Attachment.

G. Designated Record Set—Protected Health Information. If, on behalf of STATE, CONTRACTOR maintains a complete or partial designated record set, as defined in 45 C.F.R. § 164.501, upon request by STATE, CONTRACTOR shall:

1. Provide the means for an individual to access, inspect, or receive copies of the individual's Protected Health Information.

2. Provide the means for an individual to make an amendment to the individual's Protected Health Information.

3. Provide the means for access and amendment in the time and manner that complies with HIPAA or as otherwise directed by STATE.

H. Access to Books and Records, Security Audits, and Remediation. CONTRACTOR shall conduct and submit to audits and necessary remediation as required by this Section to ensure compliance with all Applicable Safeguards and the terms of the Contract and this Attachment.

1. CONTRACTOR represents that it has audited and will continue to regularly audit the security of the systems and processes used to provide services under the Contract and this Attachment, including, as applicable, all data centers and cloud computing or hosting services under contract with CONTRACTOR. CONTRACTOR will conduct such audits in a manner sufficient to ensure compliance with the security standards referenced in this Attachment.

2. This security audit required above will be documented in a written audit report which will, to the extent permitted by applicable law, be deemed confidential security information and not public data under the Minnesota Government Data Practices Act, Minn. Stat. § 13.37, subd. 1(a) and 2(a).

3. CONTRACTOR agrees to make its internal practices, books, and records related to its obligations under the Contract and this Attachment available to STATE or a STATE designee upon STATE's request for purposes of conducting a financial or security audit, investigation, or assessment, or to determine CONTRACTOR's or STATE's compliance with Applicable Safeguards, the terms of this Attachment and accounting standards. For purposes of this provision, other authorized government officials includes, but is not limited to, the Secretary of the United States Department of Health and Human Services.

4. CONTRACTOR will make and document best efforts to remediate any control deficiencies identified during the course of its own audit(s), or upon request by STATE or other authorized government official(s), in a commercially reasonable timeframe.

I. Documentation Required. Any documentation required by this Attachment, or by applicable laws, standards, or policies, of activities including the fulfillment of requirements by CONTRACTOR, or of other matters pertinent to the execution of the Contract, must be securely maintained and retained by CONTRACTOR for a period of six years from the date of expiration or termination of the Contract, or longer if required by applicable law, after which the documentation must be disposed of consistent with Section 2.6 of this Attachment.

CONTRACTOR shall document disclosures of Protected Health Information made by CONTRACTOR that are subject to the accounting of disclosure requirement described in 45 C.R.F. 164.528, and shall provide to STATE such documentation in a time and manner designated by STATE at the time of the request.

J. Requests for Disclosure of Protected Information. If CONTRACTOR or one of its Agents receives a request to disclose Protected Information, CONTRACTOR shall inform STATE of the request and coordinate the appropriate response with STATE. If CONTRACTOR discloses Protected Information after coordination of a response with STATE, it shall document the authority used to authorize the disclosure, the information disclosed, the name of the receiving party, and the date of disclosure. All such documentation shall be maintained for the term of the Contract and shall be produced upon demand by STATE.

K. Conflicting Provisions. CONTRACTOR shall comply with all applicable provisions of HIPAA and with the Contract and this Attachment. To extent that the parties determine, following consultation, that the terms of this Attachment are less stringent than the Applicable Safeguards, CONTRACTOR must comply with the Applicable Safeguards. In the event of any conflict in the requirements of the Applicable Safeguards, CONTRACTOR must comply with the most stringent Applicable Safeguard.

L. Data Availability. CONTRACTOR, or any entity with legal control of any protected information provided by STATE, shall make any and all protected information under the Contract and this Attachment available to STATE upon request within a reasonable time as is necessary for STATE to comply with applicable law.

2.3 Data Security.

A. STATE Information Management System Access. If STATE grants CONTRACTOR access to Protected Information maintained in a STATE information management system (including a STATE "legacy" system) or in any other STATE application, computer, or storage device of any kind, then CONTRACTOR agrees to comply with any additional system- or application-specific requirements as directed by STATE.

B. **Electronic Transmission.** The parties agree to encrypt electronically transmitted Protected Information in a manner that complies with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; 800-113, Guide to SSL VPNs, or others methods validated under Federal Information Processing Standards (FIPS) 140-2.

C. **Portable Media and Devices.** The parties agree to encrypt Protected Information written to or stored on portable electronic media or computing devices in a manner that complies with NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices.

2.4 CONTRACTOR Permitted Uses and Responsibilities.

A. **Management and Administration.** Except as otherwise limited in the Contract or this Attachment, CONTRACTOR may:

1. Use Protected Health Information for the proper management and administration of CONTRACTOR or to carry out the legal responsibilities of CONTRACTOR.

2. Disclose Protected Health Information for the proper management and administration of CONTRACTOR, provided that:

    a. The disclosure is required by law; or

    b. The disclosure is required to perform the services provided to or on behalf of STATE or the disclosure is otherwise authorized by STATE, and CONTRACTOR:

        i. Obtains reasonable assurances, in the form of a data sharing agreement, from the entity to whom the Protected Health Information will be disclosed that the Protected Health Information will remain confidential, and will not be used or disclosed other than for the contracted services or the authorized purposes; and

        ii. CONTRACTOR requires the entity to whom Protected Health Information is disclosed to notify CONTRACTOR of any compromise to the confidentiality of Protected Health Information of which it becomes aware.

B. **Notice of Privacy Practices.** If CONTRACTOR's duties and responsibilities require it, on behalf of STATE, to obtain individually identifiable health information from individual(s), then CONTRACTOR shall, before obtaining the information, confer with STATE to ensure that any required Notice of Privacy Practices includes the appropriate terms and provisions.

C. **De-identify Protected Health Information.** CONTRACTOR may use Protected Health Information to create de-identified Protected Health Information provided that CONTRACTOR complies with the de-identification methods specified in 45 C.F.R. § 164.514.

D. Aggregate Protected Health Information. CONTRACTOR may use Protected Health Information to perform data aggregation services for STATE. The use of Protected Health Information by CONTRACTOR to perform data analysis or aggregation for parties other than STATE must be expressly approve by STATE.

2.5 STATE Data Responsibilities

A. STATE shall disclose Protected Information only as authorized by law to CONTRACTOR for its use or disclosure.

B. STATE shall obtain any consents or authorizations that may be necessary for it to disclose Protected Information with CONTRACTOR.

C. STATE shall notify CONTRACTOR of any limitations that apply to STATE's use and disclosure of Protected Information that would also limit the use or disclosure of Protected Information by CONTRACTOR.

D. STATE shall refrain from requesting CONTRACTOR to use or disclose Protected Information in a manner that would violate applicable law or would be impermissible if the use or disclosure were performed by STATE.

2.6 Obligations of CONTRACTOR Upon Expiration or Cancellation of the Contract. Upon expiration or termination of the Contract for any reason:

A. CONTRACTOR shall retain only that Protected Health Information which is necessary for CONTRACTOR to continue its proper management and administration or to carry out its legal responsibilities, and maintain appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to electronic Protected Health Information to prevent the impermissible use or disclosure of any retained Protected Health Information for as long as CONTRACTOR retains the Protected Health Information.

B. For all other Protected Information, in compliance with the procedures found in the Applicable Safeguards listed in Section 2.1, or as otherwise required by applicable industry standards, or directed by STATE, CONTRACTOR shall immediately, destroy or sanitize (permanently de-identify without the possibility of re-identification), or return in a secure manner to STATE all Protected Information that it still maintains.

C. CONTRACTOR shall ensure and document that the same action is taken for all Protected Information shared by STATE that may be in the possession of its contractors, subcontractors, or agents. CONTRACTOR and its contractors, subcontractors, or agents shall not retain copies of any Protected Information.

D. In the event that CONTRACTOR cannot reasonably or does not return or destroy Protected Information, it shall notify STATE of the specific laws, rules or policies and specific circumstances applicable to its retention, and continue to extend the protections of the Contract and this Attachment and take all measures possible to limit further uses and disclosures of the client data for so long as CONTRACTOR or its contractors, subcontractors, or agents maintain the Protected Information.

E. CONTRACTOR shall document and verify in a report to STATE the disposition of Protected Information. The report shall include at a minimum the following information:

1. A description of all such information and the media in which it has been maintained that has been sanitized or destroyed, whether performed internally or by a service provider;

2. The method by which, and the date when, the data and media were destroyed, sanitized, or securely returned to STATE; and

3. The identity of organization name (if different than CONTRACTOR), and name, address, and phone number, and signature of individual, that performed the activities required by this Section.

F. Documentation required by this Section shall be made available upon demand by STATE.

G. Any costs incurred by CONTRACTOR in fulfilling its obligations under this Section will be the sole responsibility of CONTRACTOR.

3. INSURANCE REQUIREMENTS

3.1 **Network Security and Privacy Liability Insurance.** CONTRACTOR shall, at all times during the term of the Contract, keep in force a network security and privacy liability insurance policy. The coverage may be endorsed on another form of liability coverage or written on a standalone policy.

CONTRACTOR shall maintain insurance to cover claims which may arise from failure of CONTRACTOR's security resulting in, but not limited to, computer attacks, unauthorized access, disclosure of not public data including but not limited to confidential or private information, transmission of a computer virus or denial of service. CONTRACTOR is required to carry the following **minimum** limits:

$2,000,000 per occurrence
$2,000,000 annual aggregate

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK.