MEMORANDUM OF UNDERSTANDING

BETWEEN THE STATE OF NEW JERSEY
DEPARTMENT OF HUMAN SERVICES

And

_____

REGARDING

THE ADMINISTRATION OF DMAHS PROGRAMS INCLUDING THE NEW JERSEY MEDICAID AND CHILDREN'S HEALTH INSURANCE PROGRAMS

****

WHEREAS, the Department of Human Services ("DHS") and the _____ County Social Service Agency (the "CSSA"), (together the "Parties") desire to enter into a Memorandum of Understanding ("MOU") for the purposes set forth below; and

WHEREAS, DHS is the single State agency (42 USC 1396a(a)(5) and N.J.S.A.30:4D-5) responsible for administering, through the Division of Medical Assistance and Health Services ("DMAHS"), New Jersey's Medicaid Program and Children's Health Insurance Program ("CHIP") in accordance with 42 U.S.C. 1396a, 42 U.S.C. 1397aa, N.J.S.A. 30:4D-1 et seq., N.J.S.A. 30:4J-9 et seq. and N.J.A.C. 10:49-1.1 (these programs are commonly referred to as "NJ FamilyCare" programs); and

WHEREAS, DHS, through DMAHS, is permitted to delegate the authority to make eligibility determinations to government agencies, in accordance with 42 C.F.R. 431.10, N.J.S.A. 30:4D-7, N.J.S.A. 30:4J-12 and N.J.A.C. 10:49-1.2(a); and

WHEREAS, the CSSA has been responsible for performing certain functions, including eligibility determinations, in order to assist DHS in its responsibility to administer the Medicaid and CHIP programs, in accordance with the Medicaid State Plan and the CHIP State Plan and any waivers or demonstration projects, the current and future State Appropriations Act, the applicable provisions of State and federal law including N.J.A.C. 10:49-1.1 et seq., N.J.A.C. 10:69-1.1 et seq., N.J.A.C. 10:70-1.1 et seq., N.J.A.C. 10:71-1.1 et seq., N.J.A.C. 10:72-1.1 et seq., N.J.A.C. 10:78-1.1 et seq., N.J.A.C. 10:79-1.1 et seq., any federal State Health Official Letter, New Jersey Medicaid Communications or other official policy guidance; and

WHEREAS, Medicaid and CHIP implementing regulations at 42 C.F.R. 431.300 et seq., 42 C.F.R. 457.1110, 45 C.F.R. 155.260 and N.J.A.C. 10:49-9.7 require that all Medicaid

and CHIP beneficiary and applicant information (including information about other individuals that is included with an application) is confidential and must be carefully safeguarded; furthermore, other federal and State confidentiality statutes and rules require careful safeguarding of applicant and beneficiary protected health information ("PHI"), personally identifiable information ("PII"), Social Security records, and federal tax information (FTI); and

WHEREAS, DHS is responsible for exercising oversight of the CSSA and instituting corrective action as needed, in accordance with 42 C.F.R. 431.10(c); and

WHEREAS, DHS is responsible for maintaining a CHIP accounting system that is in compliance with federal law, in accordance with 42 C.F.R. 457.226; and

WHEREAS, the Parties seek to enter into a written agreement memorializing the Parties' responsibilities and expectations, in accordance with 42 C.F.R. 431.10(d); and

WHEREAS, this MOU memorializes the Parties' responsibilities and procedures for administering New Jersey's medical assistance programs and CHIP, in accordance with State and federal law, and all prior MOUs with DMAHS for the administration of the Medicaid program and for "Medicaid application/redetermination processing" are suspended;

NOW, THEREFORE, the Parties mutually agree as follows:

1. TERM and TERMINATION: This MOU shall be for a one-year term unless terminated or extended as set forth below:

   This Agreement may be terminated by mutual agreement in writing by both Parties.
   a. Both Parties agree that should this MOU be terminated prior to the expiration of its term, both Parties will work together as needed so that both Parties may remain in compliance with the requirements of State and federal law.
   b. Any termination of this MOU shall be without prejudice to any obligations or liabilities of the Parties accrued prior to such termination. All funds expended are accountable through the cost allocation system.
   c. This MOU may be extended by both Parties agreeing in writing to extend the MOU for two (2) additional annual terms.
   d. DMAHS may at any time unilaterally amend Appendices with 30 days of notice provided to the CSSA and without requiring an amendment of the entire MOU when needed for compliance with State or federal requirements, or for emergent circumstances.

2. MEDICAID AND CHIP ADMINISTRATION: The CSSA agrees to be responsible for performing certain functions in assisting DHS's administration of New Jersey's medical assistance and subsidized health insurance programs, including but not limited to, timely eligibility determinations and related activities (including fair hearings) for the administration of CHIP and Medicaid. It is understood that the CSSA will not be responsible for cases that are the sole responsibility of other entities such as the Social Security Administration or DMAHS's Health Benefits Coordinator (currently Conduent, formerly Xerox State Healthcare LLC). As part of the performance of these functions,

the CSSA agrees:

a. to submit an annual budget. Included in the CSSA's budget submission will be a roster including only the staff that the CSSA is counting in its budget as full (100%) time dedicated to performing Medicaid work to ensure timely and accurate processing of cases. See Appendix A Roster Template. In addition, examples of items to be in the budget to be submitted by the CSSA to DMAHS for approval shall include, but not be limited to, salaries and wages, travel expenses, office space expense, and allocation of administrative expenditures. The CSSA will not be paid for any expenses included in its calendar year budget until such budget has been approved by the DMAHS. Upon approval, the CSSA shall be responsible for the non-federal share of any approved budget expenditures. Caseload, full time employees (FTEs), budget, and work product will be reviewed quarterly by DMAHS fiscal staff;
b. that its eligibility determinations will be performed within applicable time requirements (except in unusual circumstances, eligibility must be determined within 45 days unless the person applies for Medicaid on the basis of disability in which case the time frame is 90 days maximum) and conform with 42 CFR 431.10(c)(3). Unusual circumstances must be documented in the Worker Portal and include, for example: (1) when the agency cannot reach a decision because the applicant or an examining physician delays or fails to take required action, or (2) an administrative or other emergency beyond the agency's control. If an unusual circumstance is not documented in the Worker Portal, the case will be included in the CSSA's processing times;
c. to be paid consistent with DMAHS's Eligibility Determination Incentive and Penalty Payment Program: In accordance with P.L. 2019, c.246, payments will be made quarterly as set forth in Appendix B to this MOU based on average county-specific statistics using DMAHS reports and system capabilities;
d. to use the Worker Portal to process MAGI and ABD eligibility;
e. to use the Worker Portal to timely enter applications (including paper applications) within three (3) business days;
f. to use the Worker Portal to timely update each application's status as described in Appendix B;
g. the CSSA is required to use only approved written communications such as standardized letters in the Worker Portal and notices and applications as set forth by DMAHS;
h. that all paper applications including all supporting paper documentation that was used to determine eligibility will be timely scanned into the current document imaging system. Paper applications and redeterminations, all verifications, MAGI determinations, worker case notes regarding the determination, and anything else relevant to the case determination not in the worker portal will be scanned into the document imaging system. All documents will be scanned into the document imaging system according to the guidance provided by DMAHS;
i. to enter into a corrective action plan delineating measurable outcomes and deadlines for improvements if requirements in this MOU are not performed; and
j. that the CSSA shall be responsible for any retraction of any payments due to federal eligibility audit findings on cases processed after April 1, 2021 for any case deemed ineligible. Any recoupment shall not exceed 50% of the total incentive payment awarded to the CSSA for the calendar year in which any cases improperly deemed

eligible were found. The recoupment will be applied to the CSSA as an adjustment to payment due for the following calendar year.

3. COMPLIANCE WITH LAW AND OFFICIAL GUIDANCE: Pursuant to 42 C.F.R. 431.10(d), DMAHS must have an agreement with the CSSA for determining eligibility. This agreement must set forth the relationship and respective responsibilities of the parties, the quality control and oversight of DMAHS including instituting corrective action, and that the CSSA will comply with all Medicaid requirements in carrying out its eligibility functions including complying with all relevant federal and State laws, regulations and policies, such as those related to the eligibility criteria applied by the agency under 42 CFR part 435, prohibitions against conflicts of interest and improper incentives, and safeguarding confidentiality. Consistent with this federal requirement, the CSSA agrees to assist in DHS's administration of the Medicaid and CHIP programs in accordance with the Medicaid State Plan and CHIP State Plan and any waivers or demonstration projects (and any amendments), the current and future State Appropriations Act, the applicable provisions of State and federal law including N.J.A.C. 10:49-1.1 et seq., N.J.A.C. 10:69-1.1 et seq., N.J.A.C. 10:70-1.1 et seq., N.J.A.C. 10:71-1.1 et seq., N.J.A.C. 10:72-1.1 et seq., N.J.A.C. 10:78-1.1 et seq., N.J.A.C. 10:79-1.1 et seq., as these laws may be amended, any federal State Health Official Letter, New Jersey Medicaid Communications or other DHS or CMS official policy guidance, and any future regulations promulgated under federal or State law.

   a. NATIONAL VOTER REGISTRATION ACT (NVRA): The CSSA shall comply with the voter registration agency requirements of the NVRA as required by law (52 USC 20506; N.J.S.A. 19:31-6.11; N.J.S.A. 30:4D-19.1), Medicaid Communication guidance, and any settlement DHS or DMAHS enters into related to compliance with the NVRA. The CSSA will keep records of voter registration activities and interactions as requested by DMAHS (including number of voter registration opportunity forms and applications mailed, the number of opportunity forms received back and what they state, and the number of completed voter registration applications sent to the Division of Elections or a County Elections Office) and timely report to DMAHS each quarter the NVRA statistics required by the New Jersey Division of Elections. The CSSA will not include completed voter registration documents with an individual's eligibility file.

   b. NON-DISCRIMINATION NOTICES: The CSSA agrees to incorporate DHS-approved non-discrimination statements in all eligibility notices, and maintain the non-discrimination poster in public areas of its office at all times. (See section 1557 of the Patient Protection and Affordable Care Act for the federal requirements on medical assistance and other programs.)

   c. Consistent with 45 CFR 92.1 et seq., CSSAs shall provide appropriate auxiliary aids and services, including qualified interpreters for individuals with disabilities and information in alternate formats free of charge and in a timely manner as necessary to ensure equal opportunity to participate in NJ FamilyCare. The CSSA shall also provide language assistance services, including translated documents and oral interpretation, free of charge and in a timely manner, when such services are necessary to provide meaningful access to individuals with limited English

proficiency. Upon request, DMAHS will assist the CSSA when possible to provide the alternate formats and translated documents.

4. PRIVACY, CONFIDENTIALITY and DATA SECURITY MEASURES:

   a. PRIVACY AND CONFIDENTIALITY: The CSSA acknowledges that Social Security Administration (SSA) records and Federal Tax Information (FTI) records, as well as Medicaid and CHIP records, are confidential and require safeguarding. The CSSA agrees that it will not disclose SSA or FTI records even when authorized by the beneficiary and will use these records only for determining eligibility. The CSSA will advise all staff that failure to safeguard SSA and FTI records can subject the CSSA, its employees and its workforce to civil and criminal sanctions under federal and State laws. The CSSA agrees to keep all applicant and beneficiary information for DMAHS's programs (including information about an individual not applying that is necessary for the application of another person) confidential and will use appropriate physical, technical and administrative safeguards to protect the privacy and security of such information consistent with 42 C.F.R. 431.300 et seq., 42 C.F.R. 457.1110, 45 C.F.R. 155.260 and N.J.A.C. 10:49-9.7 and other applicable federal or State statutes and rules requiring safeguarding including those laws and requirements set forth in Appendix C. The CSSA agrees to enact and maintain safeguards necessary to protect these records and prevent the unauthorized or inadvertent access to, duplication of, or disclosure of a SSA records, FTI records and any applicant or beneficiary personally identifiable information consistent with Appendix C.

   b. DATA SECURITY MEASURES: The CSSA agrees to establish, maintain, comply with and use the most current privacy and security measures to protect DMAHS applicant and beneficiary information and data as set forth in Appendix C. DMAHS agrees to provide resources to the CSSA to assist with compliance activities.

5. TRAINING AND TECHNICAL ASSISTANCE: DMAHS's Office of Eligibility Policy and its field staff will provide assistance and guidance related to eligibility determinations by the CSSA, and will provide certain eligibility training for CSSA trainers as necessary. The CSSA shall have staff trainers to provide DMAHS's trainings to the CSSA staff. The CSSA shall be responsible for timely training of all CSSA users and workforce, maintaining records of such training, and promptly training new staff as needed for activities performed under this MOU. The CSSA agrees to provide Eligibility and County Operations training to CSSA staff as needed. The CSSA agrees to provide all annual or biennial training to CSSA Users and CSSA staff including:
   - Biennial NVRA training after initial training (within 60 days of start date);
   - Annual HIPAA privacy training;
   - Annual securing the workplace training;
   - Annual IRS training in FTI ; and
   - Any other training required by County, State or federal government for the functions performed by the CSSA.

6. QUALITY CONTROL: The CSSA agrees to provide files requested by DMAHS's Bureau of Quality Control, and respond to emailed 551B letters outlining findings in case reviews within 10 days of receipt of the 551B letter. The CSSA agrees to scan case files into the document imaging system within 10 days of request from DMAHS.

   The CSSA agrees to comply with DMAHS's quality control and oversight including any reporting requirements as directed by DMAHS, in accordance with 42 CFR 431.10(d)(2); Failure to comply timely will forfeit the CSSA's opportunity to have errors and deficiencies reversed.

7. ADDITIONAL AGREEMENTS: The Parties may enter into additional agreements with each other that supplement this MOU, including agreements on inter-agency payments and specific procedures to effectuate and accomplish the purposes of this MOU.

8. RECORDS: The books, records, documents, financial statements and accounting procedures and practices of the CSSA or any subcontractor relevant to this MOU shall be subject to inspection, examination and audit by the State, DHS, DMAHS, the N.J. Department of Law and Public Safety, the N.J. Office of the State Comptroller, the Office of Legislative Services, the Comptroller General of the United States, the Internal Revenue Services, the Social Security Administration, the U.S. Department of Health and Human Services, or any authorized agents of those entities, and any other entity authorized by law to review such records. The CSSA shall maintain, retain and dispose of its records in accordance with the records retention schedule entitled "State of New Jersey County Welfare Departments & Board of Social Services (C980000-008)" issued by the New Jersey Division of Archives and Record Management.

9. NO ASSIGNMENT: The CSSA shall not assign, subcontract, transfer, or delegate any rights or responsibilities under this MOU without the prior and ongoing written consent of DMAHS. In limited circumstances, the CSSAs may be permitted to utilize outside entities (such as subcontractors or a designated Regional Health Hub (RHH)) to perform discrete and specified tasks, such as outreach to members, in an effort to further facilitate and enhance the purpose of this MOU. However, prior written approval is required from DMAHS to ensure that all eligibility requirements are met, and data privacy and security agreements are executed and in place prior to any information or data being exchanged.

10. INVALIDITY: In the event that any provision of this MOU is rendered invalid or unenforceable by any federal or State law, or State or federal court with jurisdiction, said provision(s) hereof will be immediately void and may be re-negotiated for the sole purpose of rectifying the non-compliance. The remainder of the provisions of this MOU that are not in question shall remain in full force and effect.

11. PERFORMANCE: Failure by either party to exercise any right or demand performance of any obligation under this MOU shall not be deemed a waiver of such right or obligation.

12. GOVERNING LAW: This MOU shall be construed and interpreted according to the laws of the State of New Jersey.

13. ENTIRE UNDERSTANDING: This MOU constitutes the entire understanding among the Parties and may only be modified by a written amendment signed by the Parties. Neither Party has made representations, warranties, or promises outside of this MOU. This MOU takes precedence over any other documents that may be in conflict with it.

14. PURPOSE, AMENDMENT, THIRD PARTY BENEFICIARIES: This MOU is being entered into for the sole purpose of evidencing the mutual understanding and intention of the parties. It may be amended, modified, and supplemented at any time by mutual consent in writing signed by the Parties. There are no third-party beneficiaries of this MOU.

15. COUNTERPARTS: This MOU may be executed in counterpart on separate signature pages and each fully-signed MOU shall beenforceable.

16. ENTIRETY OF AGREEMENT and SIGNATURES.
    This MOU represents the entire agreement between the Parties and supersedes all prior and contemporaneous agreements, negotiations, representations, whether written or oral, relating to its subject matter.

    The persons signing below represent and certify that each has the right and authority to execute this MOU on behalf of their respective Parties and no further approvals are necessary to create a binding agreement. This Agreement may be executed by electronic means. Each signatory who electronically signs this document agrees that their electronic signature has the same legal validity and effect as their handwritten signature on the document, and that it has the same meaning as their handwritten signature.

THEREFORE, the Parties hereto have caused this MOU to be signed on the dates set forth below:

Signed:_____ Date_____

CSSA Director's Name:_____CSSA: _____

Signed:_____ Date_____
Gregory Woods, Assistant Commissioner
Division of Medical Assistance & Health Services,
New Jersey Department of Human Services

APPENDIX A
TO THE
MOU BETWEEN DHS AND CSSA REGARDING
THE ADMINISTRATION OF DMAHS PROGRAMS INCLUDING
THE NEW JERSEY MEDICAID AND CHILDREN'S HEALTH
INSURANCE PROGRAMS

Dedicated Medicaid Staff Roster
Required form to be submitted with signed MOU

Fill in the staff roster below with only the staff whose full (100%) time is dedicated to performing Medicaid work, including full name, title and Worker Portal User ID; if none, indicate "none" or "n/a" in the roster below. DMAHS has provided a list of active users in the Worker Portal. For personnel submitted that do not have a User ID, you will be asked to provide a reason. If the CSSA intends to hire additional full-time staff this budget year, indicate each vacancy by title on the Roster.

	First Name	Last Name	Worker Portal ID	Title	Comment	Active (Y/N)
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						
30						
31						
32						

	First Name	Last Name	Worker Portal ID	Title	Comment	Active (Y/N)
33						
34						
35						
36						
37						
38						
39						
40						
41						
42						
43						
44						
45						
46						
47						
48						
49						
50						
51						
52						
53						
54						
55						
56						
57						
58						
59						
60						
61						
62						
63						
64						
65						
66						
67						
68						
69						
70						
71						
72						
73						
74						
75						
76						
77						
78						
79						

	First Name	Last Name	Worker Portal ID	Title	Comment	Active (Y/N)
80						
81						
82						
83						
84						
85						
86						
87						
88						
89						
90						
91						
92						
93						
94						
95						
96						
97						
98						
99						
100						
101						
102						
103						
104						
105						
106						
107						
108						
109						
110						
111						
112						
113						
114						
115						
116						
117						
118						
119						
120						
121						
122						
123						
124						
125						

	First Name	Last Name	Worker Portal ID	Title	Comment	Active (Y/N)
126						
127						
128						
129						
130						
131						
132						
133						
134						
135						
136						
137						
138						
139						
140						
141						
142						
143						
144						
145						
146						
147						
148						
149						
150						
151						
152						
153						
154						
155						
156						
157						
158						
159						
160						
161						
162						
163						
164						
165						
166						
167						
168						
169						
170						
171						

CALENDAR YEAR 2026 APPENDIX B
TO THE
MOU BETWEEN DHS AND CSSA REGARDING
THE ADMINISTRATION OF DMAHS PROGRAMS INCLUDING
THE NEW JERSEY MEDICAID AND CHILDREN'S HEALTH
INSURANCE PROGRAMS

DMAHS Eligibility Determination Incentive and Penalty Payment Program

Effective January 1, 2026, and continuing until DMAHS notifies the CSSA in writing of a new Eligibility Determination Incentive and Penalty Payment Program and modification to this Appendix B, the DMAHS Eligibility Determination Incentive and Penalty Payment Program shall be as follows:

Payments to be counted toward the calendar year 2026 will be based on performance incentives achieved during the period of January 1, 2026 through December 31, 2026 (under this MOU). For accounting purposes, the last quarter incentive payments will be tabulated utilizing data available to the DMAHS as of December 15, 2026. The provisions of this 2026 incentive are defined as follows:

1. Redetermination Timeliness (Incentive #1)
    a) The redetermination report in DMAHS's Shared Data Warehouse will be used for the calculation of the completed redetermination rate and the calculation will be based on the average monthly completed redeterminations during the entire quarter. As in prior years, the calculation used each month to determine the quarterly average is the number of cases on the first day of the subsequent month with a future redetermination date divided by the total cases under that CSSA's supervision. That percentage will then be used to determine the qualifying "per case" amount the CSSA will be paid for that quarter. For example, if a CSSA has 92 cases with a future redetermination date and 100 cases under its supervision, then the redetermination percentage for that month would be 92/100 or 92%. The quarterly incentive payments made to the CSSAs would then be calculated at the per case incentive that the CSSA earned (based on quarterly percentage) multiplied the number of cases the CSSA determined eligible that quarter. Payment will be made depending on the CSSA's performance with respect to timely redetermination for the quarter, as follows:
        - 95% or greater: $50 for each eligible case
        - 90% or greater but less than 95%: $40 for each eligible case
        - 85% or greater but less than 90%: $30 for each eligible case
        - 80% or greater but less than 85%: $20 for each eligible case
        - Less than 80%: $10 for each eligible case
        - Example:
            - April redetermination percentage: 96%
            - May redetermination percentage: 94%
            - June redetermination percentage: 94%

            - Average for quarter: (96+94+94)/3 = **94.67%**
            - **94.67% qualifies CSSA for $40 per eligible case**

    b) The average quarterly value will not be rounded.

c) This incentive is available only if there are no redeterminations 2 years or greater past due for that CSSA.

2. Initial/New Application Processing Time (Incentive #2)
   a) The percent calculation is based on the Integrated Eligibility System (IES)/Worker Portal report. The totals from the monthly reports will be added together in order to determine the percent of ABD cases processed within federal guidelines each quarter as compared to total cases processed each quarter and MAGI cases processed within federal guidelines each quarter as compared to total cases processed each quarter. The quarterly percentage will determine the bonus amount each CSSA will qualify for that specific quarter.
   b) From January 1, 2026 through December 31, 2026, bonus payments will be made as follows based on processing initial applications within federal guidelines:
      - $0 per quarter will be paid to CSSAs below 80%
      - $25,000 per quarter will be paid to CSSAs at or above 80% and below 90%
      - $50,000 per quarter will be paid to CSSAs at or above 90% and below 99%
      - $75,000 per quarter will be paid to CSSA at 99% or greater.
   c) This incentive is available only if processing times are met for both MAGI and ABD cases for the quarter. In other words, a CSSA would only qualify if both MAGI and ABD percentages are 80% or greater. For example, if a CSSA was at 82% for MAGI and 93% for ABD, then the CSSA would qualify for the $25,000 bonus for that quarter since that was the minimum bonus that both MAGI and ABD case processing qualified for. If either ABD or MAGI are below 80%, the CSSA would not qualify for a quarterly bonus. For CSSAs that do not process both MAGI and ABD cases, those CSSAs will receive 50% of the bonus amount they qualify for based upon their processing of ABD cases.
   d) This incentive is only available to those CSSAs who are compliant with the worker portal provisions as described in Section 2 of this MOU. Demonstration of proper use of the portal shall include but not be limited to: processing all initial and renewal applications in the portal (as functionality is made available); use of standardized notices; electronic verifications and updating of case notes as appropriate.

3. Redistribution Bonus Pool Incentive (Incentive #3)
   a) At the end of the calendar year, any unspent funding will be made available to CSSAs that achieved 90% or greater in accordance with the Redetermination Timeliness (Incentive #1) and/or Initial/New Application Processing Time (Incentive #2).
   b) CSSAs will be eligible for payment out of this bonus pool for each quarter that they qualified for a 90% or better incentive amount. For CSSAs that are at or above 90% for one incentive and below 90% for the other incentive during the quarter, only the cases associated with the qualifying incentive shall count toward redistribution pool calculations and eligibility.
   c) The payment for each qualifying CSSA will be based on the number of cases processed by that CSSA in the quarters for which they achieved 90% or greater.
   d) Example of bonus payment calculation. Assumptions in this example are:
      - $900,000 left over at the end of calendar year 2026
      - 5 CSSAs achieved 90% or greater for at least one quarter during the calendar year These 5 CSSAs had a total number of cases during qualifying quarters of 60,000
      - Bonus payment per case would be $15.00 = ($900,000 / 60,000 cases)
      - Bonus Payment will be paid at year end after all quarterly incentive payments have been made

	Cases Processed					Bonus per Case	Bonus Payment
	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Total		
CSSA 1	9,000	9,200	DNQ	DNQ	18,200	$15.00	$273,000
CSSA 2	4,500	DNQ	DNQ	4,300	8,800	$15.00	$132,000
CSSA 3	5,000	5,200	5,300	5,500	21,000	$15.00	$315,000
CSSA 4	DNQ	DNQ	3,000	3,100	6,100	$15.00	$91,500
CSSA 5	DNQ	DNQ	DNQ	5,900	5,900	$15.00	$88,500
Total	18,500	14,400	8,300	18,800	60,000	$15.00	$900,000

*DNQ means the CSSA did not qualify (achieve 90% or greater) for that specific quarter

For MOUs completed and executed by the CSSAs, and received by DMAHS after February 14, 2026, incentive payments will not be earned and paid until the quarter following the one in which the signed MOU is received by the State. The table below shows what quarters a CSSA would be eligible for payment depending upon the date of the executed agreement:

Completed and Executed by CSSA	Quarter 1	Quarter 2	Quarter 3	Quarter 4
On or before 2/14/26	Eligible	Eligible	Eligible	Eligible
2/15/26-3/31/26	Not Eligible	Eligible	Eligible	Eligible
4/1/26-6/30/26	Not Eligible	Not Eligible	Eligible	Eligible
7/1/26-9/30/26	Not Eligible	Not Eligible	Not Eligible	Eligible
10/1/26 and later	Not Eligible	Not Eligible	Not Eligible	Not Eligible

APPENDIX C
TO THE
MOU BETWEEN DHS AND CSSA REGARDING
THE ADMINISTRATION OF DMAHS PROGRAMS INCLUDING
THE NEW JERSEY MEDICAID AND CHILDREN'S HEALTH
INSURANCE PROGRAMS

Definitions,
Privacy and Confidentiality Requirements, and
Data Security Measure To Be Followed

a. AGREEMENT DEFINITIONS:

Authorized Representative means an individual who acts on behalf of an applicant or beneficiary and meets the requirements set forth at 42 CFR 435.923.

Breach means the compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, loss of control, or any similar terms or phrases that refer to situations where persons other than authorized users, for an other than authorized purpose have access to personally identifiable information whether physical or electronic.

Federal Tax Information or FTI or Return information means information as defined under Section 6103(b)(2)(A) of the Internal Revenue Code and in Internal Revenue Service (IRS) Publication 1075, as any information collected or generated by the IRS with regard to any person's liability or possible liability under the Internal Revenue Code. It includes, but is not limited to, information, including the tax return, which IRS obtained from any source or developed through any means that relates to the potential liability of any person under the Internal Revenue Code for any tax, penalty, interest, fine, forfeiture, other imposition or offense; information extracted from a return including names of dependents or the location of business, taxpayer's name, address and identification number, information collected by the IRS about any person's tax affairs whether a return was filed, under examination, or subject to other investigation or processing, including collection activities; and information contained on transcripts of accounts.

Incident means a violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices. This includes attempts (including both failed or successful) to gain unauthorized access to a system or its data, unwanted disruption, the unauthorized use of a system for the processing or storage of data; and change 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 misroutingof mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification or destruction. Certain adverse events (e.g., floods, fires, electrical outages, excessive heat, etc.) can cause system crashes but are not considered Incidents. An Incident becomes a Breach when there is 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 to personally identifiable information or personal health information, whether physical or electronic.

PII or Personally Identifiable Information refers to information about an individual,

(1) that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and

(2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Examples of PII include, but are not limited to:

- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number
- Address information, such as street address or email address
- Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

PII includes social security numbers and social security records.

Protected Health Information or PHI means any information, including genetic information, whether oral or recorded in any form or medium, that:

(1) is created or received by a health care provider, health plan such as DMAHS or a managed care organization, or health care clearinghouse; and

(2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

b. PRIVACY AND CONFIDENTIALITY REQUIREMENTS:

SSA and FTI data about applicants and beneficiaries can only be used for determining eligibility and cannot be otherwise used or disclosed, even when authorized by the applicant or beneficiary. Disclosure of Medicaid or CHIP applicant or beneficiary information, other than SSA records and FTI, must be authorized prior to disclosure and be disclosed only to the applicant or beneficiary or their Authorized Representative, to an individual or entity that the applicant or beneficiary or their Authorized Representative authorizes to received specific information, or to those with which the CSSA has agreements to protect the privacy and security of such disclosures consistent with the standards applicable to DMAHS and for the purpose of determining eligibility under this MOU. The CSSA agrees that it will keep all applicant and beneficiary information for DMAHS's programs (including information about an individual not applying that is necessary for the application of another person)

confidential and will use appropriate physical, technical and administrative safeguards to protect the privacy and security of such information consistent with 42 C.F.R. 431.300 et seq., 42 C.F.R. 457.1110, 45 C.F.R. 155.260 and N.J.A.C. 10:49-9.7 and any other federal or State statute and rule requiring confidentiality including, but not limited to, the following:

1. The federal Medicaid Act at 42 U.S.C. 1396 et seq.; 42 C.F.R. 430 et seq.; in particular 42 U.S.C. 1396a(a)(7) and 42 C.F.R. 431.300 et seq.

2. The federal State Children's Health Insurance Program at 42 U.S.C. 1397aa et seq., and its rules at 42 C.F.R. 457, especially 42 C.F.R. 457.1110.

3. The Patient Protection and Affordable Care Act of 2010 as amended by the HealthCare and Education Reconciliation Act referred to collectively as the Affordable Care Act, and its implementing regulations at 42 C.F.R. 431, 435, 457 and 45 C.F.R. 155-157, including the privacy and security rule at 45 C.F.R. 155.260 (with penalties at 45 C.F.R. 155.285).

4. The Information Exchange Agreement between the Social Security Administration and the State of New Jersey, Department of Human Services.

5. IRS federal tax information rules at 26 U.S.C. 6103 and IRS Publication 1075.

6. The Health Insurance Portability and Accountability Act (HIPAA, codified at 42 U.S.C. 300gg et seq., and 42 U.S.C. 1320d et seq.) and Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, with regulations at 45 C.F.R. parts 160, 162, and 164.

7. Substance Use Disorder Patient Record protections at 42 U.S.C. 290dd-2 and regulations at 42 C.F.R. 2.1 et seq.

8. N.J.S.A. 26:5C-5 and -7 regarding confidentiality of AIDS or HIV infection records.

9. N.J.S.A. 9:6-8.10a regarding confidentiality of records of child abuse reports.

10. N.J.S.A. 10:5-47 regarding confidentiality of genetic testing and information, including resulting hereditary disorders as set forth in N.J.S.A. 26:5B-1 et seq.

11. N.J.S.A. 26:4-41 regarding confidentiality of sexually transmitted disease information.

12. N.J.S.A. 30:4-24.3 regarding confidentiality of services received by a client in a DHS non-corrections institution, with regulations at N.J.A.C. 10:41-2.1 and 4.1.

13. The New Jersey Medical Assistance and Health Services Act at N.J.S.A. 30:4D-1 et seq., and its rules at N.J.A.C. 10:49-1.1 et seq. In particular, the Medicaid confidentiality rule is at N.J.A.C. 10:49-9.7.

14. N.J.S.A. 44:10-47 regarding confidentiality of Supplemental Nutrition Assistance Program and for Work First New Jersey program information.

15. N.J.S.A. 54:4-2.42 regarding the confidential nature of State tax return information.

16. N.J.S.A. 56:8-161 to 164 regarding customer records and display of Social Security records

17. The Open Public Records Act (N.J.S.A. 47:1A-1 et seq).

18. The CSSA acknowledges that SSA records, information or data regarding individuals are confidential and require safeguarding. SSA records may only be used for determining eligibility for Medicaid and CHIP. Failure to safeguard SSA records can subject the CSSA and its employees and workforce to civil and criminal sanctions under federal and State laws including the Federal Privacy Act at 5 U.S.C. 552a; Social Security Act sections 205 and 1106 (see 42 U.S.C. 405(c)(2)(C)(viii) and 42 U.S.C. 1306, respectively); and N.J.S.A. 56:8-164. The CSSA shall train all workforce that SSA records can only be used for determining Medicaid and CHIP eligibility, the standard for safeguarding, the requirement of reporting breaches and improper disclosure of SSA records immediately and within 24 hours, and the penalties for improper use and disclosure. The CSSA shall ensure that all persons who will handle or have access under this MOU to any SSA records will be advised of the confidentiality of the records; the safeguarding requirements to protect the records and prevent unauthorized access, handling, duplication and re-disclosure of the SSA records; the breach reporting requirements, and the civil and criminal sanctions for failure to safeguard the SSA records (subject to SSA changes: civil penalties and costs of prosecution; criminal penalties of $5,000 and misdemeanor). The CSSA agrees to enact and/or maintain safeguards necessary to protect these records and prevent the unauthorized or inadvertent access to, duplication of or disclosure of a Social Security number or other SSA records.

c. DATA SECURITY MEASURES TO BE FOLLOWED:

The CSSA agrees to protect the privacy and security of its Medicaid and CHIP data consistent with the following security guidelines:

1. The Patient Protection and Affordable Care Act at security rule 45 CFR 155.260 requiring the Acceptable Risk Controls for Affordable Care Act, Medicaid, and Partner Entities (ARC-AMPE), https://www.cms.gov/files/document/arc-ampe-vol-1-v102-508-5cr-04112025.pdf, as published by the Centers for Medicare and Medicaid Services (CMS) which replaces "Minimum Acceptable Risk Standards for Exchanges" (MARS-E 2.2).
2. National Institute for Standards and Technology current guidance. See https://csrc.nist.gov/ .
3. The Federal Information Security Modernization Act of 2014 (this is being renamed to reflect that FISMA 2014 appears to supersede FISMA 2002): https://www.cisa.gov/federal-information-security-modernization-act.
4. State of New Jersey Office of Information Technology, Information Security

Policies, https://nj.gov/it/whatwedo/policylibrary/, as updated, and the New Jersey Office of Homeland Security and Preparedness Statewide Information Security Manual as updated, https://www.cyber.nj.gov/NJ-Statewide-Information-Security-Manual.pdf.

The CSSA agrees to use the following security measures:

5. The CSSA shall limit access to its electronic systems and to its data containing applicant and beneficiary information for DMAHS programs to only those authorized CSSA workforce members who need DMAHS applicant and beneficiary data to perform their job duties consistent with this MOU. In this Appendix C, DMAHS electronic systems and data with DMAHS applicant and beneficiary information will be referred to as "DMAHS PII." Information about applicants and beneficiaries on non-electronic records (paper, phone) is also referred to as DMAHS PII. CSSA workforce members who need to access DMAHS PII to perform their job duties under this MOU are referred to in this Appendix C as "CSSA Users."

6. The CSSA shall use appropriate administrative safeguards to protect DMAHS PII. CSSA User access limitations shall include role-based access limits. The CSSA shall have a written access policy. CSSA Users granted access to DMAHS PII shall be advised of the confidential nature of the data, the safeguards required to protect the data, and the civil and criminal sanctions for noncompliance with the confidentiality requirements contained in applicable State and federal laws. Access to DMAHS PII should always be limited to the minimum necessary to accomplish the official job duty or task. A warning banner providing notice of the confidentiality of DMAHS PII must be displayed when accessing eligibility or other DMAHS PII.

7. The CSSA shall implement and maintain appropriate physical security and storage safeguards to protect the DMAHS PII from loss, theft or inadvertent disclosure. The CSSA shall ensure that data containing DMAHS PII shall be physically and technologically secure from access by unauthorized persons during work hours and non-work hours, and when not in use (door locks, card keys, biometric identifiers, other appropriate protections.). Fax machines and printers that may receive PII shall be secured by appropriate physical barriers. DMAHS PII shall be accessed and used in such a way that unauthorized persons cannot retrieve any DMAHS PII data by means of computer, remote terminal or other means. DMAHS PII will only be transported by authorized CSSA Users. Laptops and other electronic devices and media containing DMAHS PII must encrypt and password-protect the DMAHS PII. Storing DMAHS PII on movable devices is to be avoided. Accessing DMAHS PII by CSSA Users outside of normal work locations is to be avoided. DMAHS PII should not be included in emails and further cannot be sent by email outside of the CSSA secure email system unless encryption is used (such as the State's Datamotion system). CSSA Users will only send emails containing DMAHS PII (using encryption as appropriate) to persons authorized to receive DMAHS PII at authorized email addresses. CSSA will establish appropriate safeguards for DMAHS PII by performing, and annually updating, a risk-based security assessment. In cases involving FTI, CSSA Users and agents must comply with IRS Publication 1075's rules and restrictions on use and disclosure of FTI and emailing

of FTI.

i. When sending or receiving faxes containing PII or printing documents containing PII:
   - Fax machines and printers must be located in a locked room, and for faxes, there must be a trusted staff member having custodial coverage over outgoing and incoming transmissions;
   - For faxes, accurate broadcast lists and other preset numbers of frequent fax recipients must be maintained; and
   - For faxes, a cover sheet must be used that explicitly provides guidance to the recipient that includes a notification of the sensitivity of the data and the need for protection, and a notice to unintended recipients to telephone the sender (collect if necessary) to report the disclosure and confirm destruction of the information.

8. The CSSA agrees to implement and maintain appropriate technical safeguards. The CSSA agrees that DMAHS PII will be processed under the immediate supervision and control of authorized personnel to protect the confidentiality of the data in such a way that unauthorized persons cannot retrieve any such data by means of computer, remote terminal, or other means. CSSA Users must enter personal identification numbers when accessing DMAHS PII on electronic systems. The CSSA will strictly limit authorized access to those electronic data areas necessary for CSSA Users to perform his or her official duties.

9. IRS Safeguards. For FTI, CSSA agrees to maintain all tax return information sourced from the IRS in accordance with IRC section 6103(p)(4) and comply with the safeguard requirements set forth in IRS Publication 1075, "Tax Information Security Guidelines for Federal, State and Local Agencies," which is the IRS published guidance for security guidelines and other safeguards for protecting return information pursuant to 26 C.F.R. 301.6103(p)(4)-1. In addition, IRS safeguarding requirements require the CSSA, if it receives FTI (for example, through the IEVS or Iacquire system), to:

   i. Establish a central point of control for all requests for and receipt of FTI, and maintain a log to account for all subsequent disseminations and products made with/from that information, and movement of the information until destroyed, in accordance with Publication 1075, section 3.0.
   ii. Establish procedures for secure storage of FTI consistently maintaining two barriers of protection to prevent unauthorized access to the information, including when in transit, in accordance with Publication 1075, section 4.0.
   iii. Consistently label FTI to make it clearly identifiable and to restrict access by unauthorized individuals. Any duplication or transcription of FTI creates new records which must also be properly accounted for, logged and safeguarded. FTI should not be commingled with other CSSA records unless the entire file is safeguarded in the same manner as required for FTI and the FTI within is clearly labeled in accordance with Publication 1075, section 5.0.
   iv. Restrict access to FTI solely to officers, employees, agents and contractors of the CSSA whose duties require access. Prior to access, the CSSA must

evaluate which personnel require such access. Authorized individuals may only access FTI to the extent necessary to perform services related to this MOU, in accordance with Publication 1075, section 5.0.

v. Ensure, in accordance with Publication 1075, section 5.1.1, prior to access, that officers, employees, agents or contractor personnel who require access to FTI for their job duties, successfully undergo the background investigation (including fingerprinting and criminal background check) required by IRS Publication 1075, consistent with State law (P.L. 2017, c.179), coordinated through the DHS Central Fingerprint Unit consistent with DHS policy, that it is completed for any individual who will have access to FTI, and that a reinvestigation is conducted within 10 years at a minimum. DHS Central Fingerprint Unit must also be notified when an individual no longer has access to FTI for their job duties (for example, when individuals retire or get promoted to different positions) and no longer requires updating of the background investigation required by this paragraph (CFU can be reached at 609-292-0207).

vi. Prior to initial access to FTI and annually thereafter, ensure that employees, officers, agents and contactors who will have access to FTI receive security awareness training regarding the confidentiality restrictions applicable to the FTI and certify acknowledgment in writing that they are informed of the criminal penalties and civil liability provided by section 7213, 7213A, and 7431 of the Internal Revenue Code for any willful disclosure or inspection of FTI that is not authorized by the Internal Revenue Code in accordance with Publication 1075, section 6.0.

Cooperate with DHS in DHS submitting annually a comprehensive Safeguard Security Report required by IRS Publication 1075, that fully describes the procedures established for ensuring the confidentiality of FTI; addresses all outstanding areas for improvement; accurately and completely reflects the current physical and logical environment for the receipt, storage, processing and transmission of FTI; accurately reflects the security controls in place to protect FTI in accordance with Publication 1075 and a commitment to protect FTI;

vii. Report suspected unauthorized inspection or disclosure of FTI within 24 hours of discovery to DMAHS for reporting to the IRS in accordance with Publication 1075, section 10.0, and cooperate with investigators from State or federal government, providing data and access as needed to determine the facts and circumstances of the incident; support site review to assess compliance with Publication 1075 requirements by means of manual and automated compliance and vulnerability assessment testing, including coordination with information technology divisions to secure preapproval, if needed, for automated system scanning and to support timely mitigation of identified risks to FTI in a Corrective Action Plan for as long as FTI is received or retained.

viii. Ensure that FTI is properly destroyed or returned to the IRS when no longer needed based on established CSSA record retention schedules in accordance with Publication 1075, section 8.0, or after such longer time as required by applicable law.

ix. Conduct periodic internal inspections of activities where FTI is maintained to ensure IRS safeguarding requirements are met and permit the IRS access to such facilities as needed to review the extent to which CSSA is complying

with requirements.

x. Ensure information systems processing FTI are compliant with Section 3544(a)(1)(A)(ii) of the Federal Information Security Management Act of 2002 (FIMSA). The CSSA will maintain written documentation that fully describes the systems and security controls established at moderate impact level in accordance with National Institute of Standards and Technology (NIST) standards and guidance. Required security controls for systems that receive, process, store and transmit FTI are provided in Publication 1075 section 9.0.

xi. Ensure that contracts with contractors and subcontractors performing work involving FTI under the MOU contain specific language requiring compliance with IRC section 6103(p)(4) and Publication 1075 safeguard requirements and enforce DMAHS's right, CMS's right and IRS's right to access contractor and subcontractor facilities to conduct periodic internal inspections where return information is maintained to ensure IRS safeguarding requirements are met.

xii. Officers, employees and agents who inspect or disclose FTI obtained pursuant to this MOU in a manner or for a purpose not authorized by 26 U.S.C. 6103 are subject to the criminal sanction provisions of 26 U.S.C. sections 7213 and 7213A, and 18 U.S.C. section 1030(a)(2), as may be applicable. In addition, the CSSA may be required to defend a civil damages action under section 7431. Criminal Penalties subject to IRS changes: section 7213 specifies that willful unauthorized disclosure of returns or return information by an employee or former employee is a felony. The penalty can be a fine of up to $5,000 or up to five (5) years in jail, or both, plus costs of prosecution. Under section 7213A, willful unauthorized access or inspection of taxpayer records by an employee or former employee is a misdemeanor. This applies to both paper documents and electronic information. Violators can be subject to a fine of up to $1,000 and/or sentenced to up to one year in prison. Civil Penalties subject to IRS changes: A taxpayer whose return or return information has been knowingly or negligently inspected or disclosed by an employee in violation of section 6103 may seek civil damages. Section 7431 allows a taxpayer to institute action in district court for damages where there is unauthorized inspection or disclosure. If the court finds there has been an unauthorized inspection or disclosure, the taxpayer may receive damages of $1,000 for each unauthorized access or disclosure, or actual damages, whichever is greater, plus punitive damages (in the case of willful or gross negligence), and costs of the action (which may include attorney's fees). There is no liability under section 7431 if the disclosure was the result of a good faith but erroneous interpretation of section 6103.

xiii. Allow the IRS to conduct periodic safeguard reviews of the CSSA to assess whether security and confidentiality of FTI is maintained consistent with the safeguarding protocols described in Publication 1075. Periodic safeguard reviews will involve the inspection of CSSA facilities and contractor facilities where FTI is maintained, the testing of technical controls for computer systems sorting, processing or transmitting FTI, review of CSSA recordkeeping policies and interviews of CSSA employees and contractor employees as needed to verify the use of FTI and assess the adequacy of procedures established to protect FTI.

xiv. Recognize and treat all FTI records and related communications as IRS official agency records; understand that they are property of the IRS, and that IRS records are subject to disclosure restrictions under federal law and IRS rules and regulations and may not be released publicly under the Open Public Records Act (N.J.A.C. 47:1A-1 et seq.), and that any requestor seeking access to IRS records should be referred to the federal Freedom of Information Act (FOIA) statute (5 U.S.C. 552) and the IRS. If the CSSA determines that it is appropriate to share FTI documents and related communications with another governmental entity for the purposes of operational accountability or to further facilitate the protection of FTI, that the recipient governmental entity must be made aware, in unambiguous terms, that FTI and related IRS communications are property of the IRS and that they constitute IRS official agency records, that any request for the release of IRS records is subject to disclosure restrictions under federal law and IRS rules and regulations, and that any requestor seeking access to IRS records should be referred to the federal Freedom of Information Act (FOIA) statute. Federal agencies in receipt of FOIA requests for FTI and related IRS communications must forward them to the IRS for reply.

10. IRS and DMAHS PII Incident Handling and Reporting. In regard to FTI, SSA records, and DMAHS PII, the CSSA shall comply with DHS's formal written policies and procedures for responding to privacy and security incidents, breaches and the required breach notification procedures in accordance with State and federal law, ARC-AMPE, IRS, SSA and CMS guidance. These policies and procedures will include the scope, roles, responsibilities and how to:

    i. Identify Incidents involving DMAHS PII, SSA records or FTI
    ii. Report all suspected or confirmed Incidents involving DMAHS PII, SSA records or FTI to the DMAHS Privacy Officer (currently Charles Castillo; Charles.Castillo@dhs.nj.gov) and DMAHS Information Security Officer (currently Achuta Nagireddy; achuta.nagireddy@dhs.nj.gov) immediately upon discovery. This requirement applies to all system environments (e.g., production, pre-production, test, development). Using DMAHS's Incident Reporting Form, the CSSA shall report all suspected or confirmed Incidents (including loss or suspected loss involving DMAHS PII, SSA records or FTI) to DMAHS within one (1) hour of discovery for reporting to CMS, SSA and/or the IRS as well as State officials. Privacy and security incidents include suspected or confirmed incidents that involve PII. DMAHS must report a breach or suspected breach to CMS and as required by HIPAA and as required by the New Jersey Office of Information Technology. DMAHS must also report breaches or suspected breaches involving social security numbers and records to the SSA, and DMAHS must report breaches or suspected breaches involving FTI to the IRS. DMAHS will comply with all applicable laws that require the notification of individuals in the event of unauthorized release of PII, PHI, SSA records or FTI, or other event requiring notifications under applicable law.
    iii. Work with DMAHS to determine the risk level of Incidents involving DMAHS PII, SSA records or FTI, and determine a risk-based response to such Incidents.
    iv. Work with DMAHS to determine whether breach notification is required,

and if so, work with DMAHS to identify appropriate breach notification methods, timing, source, and contents from among different options and bear costs associated with the notice as well as any mitigation.

v. Limit the disclosure of information about individuals whose information may have been compromised, misused, or changed without proper authorization, determine the person who improperly disclosed DMAHS PII, SSA records or FTI, and report to authorized federal, State, or local law enforcement investigators in connection with efforts to investigate and mitigate the consequences of any such Incidents.

11. The CSSA has and follows written policies and procedures regarding the creation, collection, use and disclosure of DMAHS PII (including SSA records and FTI) consistent with State and federal privacy and security requirements. CSSA has trained each current CSSA User and will timely train any new CSSA User in these policies including regarding State and federal Medicaid confidentiality requirements and HIPAA privacy and security requirements including workplace security and incident response, in addition to the required SSA record training and IRS training for FTI access. CSSA will annually review and update its written privacy and security policies, and annually refresh staff training in these policies.

12. The CSSA will restrict access to DMAHS PII, SSA records and FTI to officers, employees and contractors of the CSSA who have an official purpose for getting access to the data. Any contractor or agent of the CSSA shall sign an agreement with the same standards as this MOU in order to have any access to DMAHS PII, SSA records and FTI. The CSSA shall require each CSSA User requiring access to DMAHS PII (including SSA records and FTI) to sign a confidentiality agreement requiring that they maintain the confidentiality of the DMAHS PII, requiring that the CSSA User will only access DMAHS PII that is necessary for their job duties, and requiring that such records will be properly stored and destroyed when no longer needed. CSSA Users will sign an FTI confidentiality agreement agreeing to follow Publication 1075 requirements if the CSSA User has access to FTI.

13. The CSSA will not use DMAHS PII, SSA records or FTI to extract information concerning individuals for any purpose not allowed by this MOU and federal law.

14. The CSSA agrees that DMAHS PII is and will remain the property of DMAHS, SSA records are the property of SSA, and FTI records are the property of the IRS. These records will be retained and destroyed consistent with CSSA record retention policies.

15. The CSSA acknowledges that DMAHS's applications and its website will provide notice to applicants and beneficiaries of the use of an individual's PII.

16. The CSSA acknowledges and will advise CSSA Users that any individual who receives information from the CMS Federally Facilitated Marketplace (FFM) or Federal Data Services Hub (FDSH) in connection with an eligibility determination for enrollment in DMAHS's programs (including DMAHS PII provided to the CSSA under this MOU) and who knowingly and willfully uses or discloses the information in a manner or for a purpose not authorized by 45 CFR 155.260 and Section 1411(g) of the ACA, is potentially subject to the civil penalty provisions of

Section 1411(h)(2) of the ACA and 45 CFR 155.285, which carries a fine of up to $25,000.

17. The CSSA agrees to provide, pursuant to 5 U.S.C. 552(o)(1)(K), access for the Government Accountability Office (Comptroller General) to all DMAHS PII records as necessary in order to verify compliance with federal requirements.

18. The CSSA agrees that DMAHS's electronic data systems, including DMAHS PII, are as is. Any inaccuracies in DMAHS data systems that are discovered by the CSSA shall be corrected according to procedure or reported to DMAHS's Office of Eligibility Policy, if appropriate.

19. The CSSA understands that access to DMAHS PII is dependent upon the availability of the DMAHS systems functioning and there may be periods of unavailability from time to time due to system maintenance.

20. The CSSA must use either Appendix C-1 or other similar form to track unmet security measures and the plan of action to correct them. The Plan of Action form must be provided to DMAHS within 90 days of execution of the MOU whether or not the CSSA determines that certain security controls are unmet or weaknesses have been identified. If the CSSA determines that none exist, return the form with "None". The CSSA is required to update the Plan of Action annually and as necessary when security control items are identified or addressed.

APPENDIX C-1
TO THE
MOU BETWEEN DHS AND CSSA REGARDING
THE ADMINISTRATION OF DMAHS PROGRAMS INCLUDING
THE NEW JERSEY MEDICAID AND CHILDREN'S HEALTH
INSURANCE PROGRAMS

CSSA Privacy, Confidentiality and Security Plan of Action

County:	
Contact Name:	
Title:	
Email:	

Instructions:

This form is to help the CSSA track unmet security controls or weaknesses in security controls. This completed Plan of Action form must be provided to DMAHS within 90 days of execution of the MOU if the CSSA determines that certain security controls are unmet or weaknesses have been identified. The CSSA is required to update this Plan of Action annually and as necessary when security control items are identified or addressed. List each unmet security measure, identify the risk level, the corrective action needed, interim and final target dates for actions to be completed and the current status.

Risk Levels:

High Risk	A threat event could be expected to have a severe or catastrophic adverse effect on CSSA operations or assets, individuals, or other organizations.
Moderate Risk	A threat event could be expected to have a serious adverse effect on CSSA operations or assets, individuals, or other organizations.
Low Risk	A threat event could be expected to have a limited adverse effect on CSSA operations or assets, individuals, or other organizations.

Privacy, Confidentiality and Security Plan of Action					
#	Security Measure Weakness	Risk Level (H-M-L)	Action Needed	Target Completion Dates	Status (Ongoing Or Completed)

Privacy, Confidentiality and Security Plan of Action					
#	Security Measure Weakness	Risk Level (H-M-L)	Action Needed	Target Completion Dates	Status (Ongoing Or Completed)