

**INFORMATION EXCHANGE AGREEMENT
BETWEEN
THE CENTERS FOR MEDICARE & MEDICAID SERVICES
AND
MEDICAID/CHIP AGENCIES
FOR
THE DISCLOSURE OF INFORMATION FOR ADMINISTRATION OF INSURANCE
AFFORDABILITY PROGRAMS**

CMS Information Exchange Agreement No. 2019 – 03

I. PURPOSE

The purpose of this Information Exchange Agreement (IEA) (Agreement) is to establish the terms, conditions, safeguards, and procedures under which the Centers for Medicare & Medicaid Services (CMS) will exchange information with Medicaid/CHIP agencies to fulfill their respective responsibilities in administering Insurance Affordability Programs under the Patient Protection and Affordable Care Act (Public Law 111-148) as amended by the Health Care and Education Reconciliation Act of 2010 (Public Law 111-152), and as further amended, referred to collectively as the Affordable Care Act (ACA).

This Agreement establishes the terms, conditions, safeguards, and procedures under which:

- A. CMS will receive data from the state Medicaid and/or CHIP agency(ies) to verify an individual's enrollment in Medicaid or CHIP, other than enrollment for certain limited benefit packages, in states with a Federally-Facilitated Exchange or State-Based Exchange on the Federal Platform. Enrollment in Medicaid or CHIP generally constitutes minimum essential coverage
- B. CMS and the state Medicaid and/or CHIP agency(ies) will exchange information related to eligibility determinations and assessments for Insurance Affordability Programs, including the transfer of an Applicant or Enrollee's account; in states with a Federally-Facilitated Exchange or State-based Exchange on the Federal platform, this account transfer will take place through the Federal Data Services Hub (the Hub) in order to either complete the Eligibility Determination or process the enrollment as described in 42 C.F.R. § 435.1200 and 45 C.F.R. §§ 155.302 and 155.345.

The terms and conditions of this Agreement will be carried out by authorized employees and contractors of CMS and Medicaid/CHIP agencies. For each Medicaid/CHIP agency signatory to this agreement, CMS and the relevant Medicaid/CHIP agency are each a "Party" and collectively "the Parties." By entering into this Agreement, the Parties agree to comply with the terms and conditions set forth herein, and with applicable law. CMS enters into this

Agreement in its capacity operating and administering one or more Federally-Facilitated Exchange(s) and the Federal eligibility and enrollment platform in states with a State-based Exchange on the Federal platform, and in its capacity operating and administering the Hub. The state Medicaid and/or CHIP agency enters into this agreement in its capacity administering the respective program under the Social Security Act.

II. APPLICABILITY

The CMS Privacy Act System of Records, "Health Insurance Exchanges (HIX) Program" System No. 09-70-0560, as amended, supports the CMS Health Insurance Exchanges Program established under the provisions of the ACA. See 78 FR 63211 (10/23/13), 83 FR 6591 (2/14/18). The disclosures from CMS under this Agreement constitute a "routine use" as defined by the Privacy Act 5 U.S.C. § 552a(b)(3). Routine uses 1, 2, and 3 of the System of Records cover the following disclosures from CMS under this Agreement:

1. Minimum Essential Coverage Verification
2. Account Transfers

III. LEGAL AUTHORITY

This Agreement is executed in compliance with the Privacy Act of 1974 (5 U.S.C. § 552a) and its implementing regulations and guidance. The following statutory and regulatory provisions and attestations provide legal authority for the specific disclosures contemplated under this Agreement:

1. This Agreement is executed to implement certain health care reform provisions of the ACA, and regulations at 42 C.F.R. Parts 431, 435, and 457, as well as 45 CFR Parts 155-157, implementing ACA provisions and amendments to the Social Security Act.
2. Pursuant to 42 C.F.R. § 431.10(c) and 45 C.F.R. §§ 155.302, 155.305, 155.330 and 155.335, an Exchange may either:
 - a. assess an applicant or enrollee as eligible for Medicaid or CHIP or
 - b. determine the eligibility of an applicant or enrollee for Medicaid or CHIP.
3. 42 C.F.R. §§ 435.1200(d) and 457.348(c) require Medicaid and CHIP agencies to accept, via secure electronic interface, the electronic account for an individual assessed as eligible for Medicaid or CHIP by another Insurance Affordability Program, and notify such program of the receipt of the electronic account and notify such program of the final determination of eligibility made by the agency for individuals who enroll in the other insurance affordability programs pending determination of the completion of Medicaid eligibility. 45 C.F.R. §§ 155.302 and 155.345 require an Exchange to transmit to a state agency administering Medicaid or CHIP all information provided on an application and obtained or verified by the Exchange for purposes of making an Eligibility Determination when the Exchange assesses the individual as potentially eligible for Medicaid or CHIP or when the individual requests a full eligibility determination based on eligibility criteria

that are not described in 45 C.F.R. § 155.305(c).

4. 42 C.F.R. §§ 435.1200(e) and 457.350 require the Medicaid and CHIP agencies to determine potential eligibility for, and, as appropriate, transfer via a secure electronic interface the individual's electronic account to, other Insurance Affordability Programs.
5. Pursuant to 45 C.F.R. § 155.320, an Exchange must verify whether an individual is eligible for, or enrolled in Medicaid or CHIP by sending identifying information to the state Medicaid or CHIP agency. Except as noted above at I.A.1-4., eligibility for either the Medicaid or CHIP program constitutes eligibility for minimum essential coverage (as that term is defined in § 5000A(f) of the Internal Revenue Code of 1986, 26 U.S.C. § 5000A). Eligibility for minimum essential coverage precludes eligibility for APTCs and CSRs under 26 U.S.C. § 36B(c)(2) and § 1402(f) of the Affordable Care Act.
6. Section 6103(l)(21) of the Internal Revenue Code of 1986, 26 U.S.C. § 6103(l)(21), permits disclosure of certain tax Return Information for purposes of determining eligibility for certain Insurance Affordability Programs and prohibits disclosure of Federal Tax Information to an Exchange or state agency administering a state program, unless the program is in compliance with the safeguards requirements of that section, and unless the information is used to establish eligibility for certain Insurance Affordability Programs.

IV. DEFINITIONS

For purposes of this Agreement, the following definitions apply:

1. "ACA" means Patient Protection and Affordable Care Act (Public Law No. 111-148), as amended by the Health Care and Education Reconciliation Act of 2010 (Public Law No. 111-152), and as further amended.
2. "Account Transfer" means transfer of the Individual's Account by one Insurance Affordability Program to another Insurance Affordability Program in states operating under the Federally-Facilitated Exchange, as described at 42 C.F.R. §§ 435.1200, 457.348, and 457.350, and 45 C.F.R. §§ 155.302 and 155.345.
3. "Administering Entity" or "AE" means a state entity administering an Insurance Affordability Program. An AE may be a state Medicaid agency, a Children's Health Insurance Program (CHIP), a state basic health program (BHP), or a State-Based Exchange established under § 1311 of the ACA.
4. "Applicant" means an individual who is seeking eligibility for an Insurance Affordability Program or a certification of Exemption through an application.
5. "APTC" (Advanced Premium Tax Credit) means advance payments of the tax credits specified in 26 U.S.C. § 36B of the Internal Revenue Code (as added by § 1401 of the

ACA) which are provided on an advance basis on behalf of an eligible individual enrolled in a QHP through an Exchange in accordance with §§ 1411 and 1412 of the ACA.

6. “BHP” means an optional state basic health program established under § 1331 of the ACA.
7. “Breach” is defined by Office of Management and Budget (OMB) Memorandum M-07-16, Safeguarding and Responding to the Breach of Personally Identifiable Information, May 22, 2007, as the compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, loss of control, or any similar term or phrase that refers to situations where persons other than authorized users or for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.
8. “CHIP” means the state program established under Title XXI of the Social Security Act.
9. “CMS” means the Centers for Medicare & Medicaid Services.
10. “CSR” means cost-sharing reductions for an eligible individual enrolled in a silver level plan through the Exchange, or for an individual who is an eligible Indian (as defined in section 4(d) of the Indian Self-Determination and Education Assistance Act, 25 U.S.C. § 450b(d)) enrolled in a any QHP through the Exchange.
11. “Eligibility Assessment” means the verification process whereby eligibility for enrollment in a QHP through the Exchange and for APTC and CSRs are determined and an evaluation of eligibility is made for Medicaid and/or CHIP benefits, without a final Eligibility Determination for those benefits.
12. “Eligibility Determination” means the determination of eligibility for enrollment in a QHP through the Exchange and, if applicable, for Insurance Affordability Programs or certificates of Exemption from the individual shared responsibility payment. The term “Eligibility Determination” includes initial determinations, mid-year and annual Redeterminations, and Renewals, and any appeal process related to an eligibility determination.
13. “Enrollee” means a qualified individual or qualified employee enrolled in a QHP through a Exchange or in an Insurance Affordability Program.
14. “Exchange” means an American Health Benefit Exchange established under §§ 1311(b), 1311(d), or 1321(c)(1) of the ACA, including State-Based Exchanges (SBEs), including State-Based Exchanges on the Federal Platform (SBE-FPs), and FFEs.
15. “Exemption” means an exemption from the individual shared responsibility provisions under 26 U.S.C. 5000A.
16. “FFE” means Federally-Facilitated Exchange, which is an Exchange established by HHS and operated by CMS under § 1321(c)(1) of the ACA.

17. "Hub" or "Data Service Hub" is the CMS federally managed service to transmit data between Federal and State Administering Entities and to interface with Federal agency partners and data sources.
18. "Incident" is defined by OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (January 3, 2017), as an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
19. "Individual" includes both an Applicant and/or Enrollee.
20. "Individual's Account" means all information provided as a part of the application, update or Renewal that initiated the Eligibility Determination or Eligibility Assessment, and any information obtained or verified by the Administering Entity relevant to the Eligibility Assessment or Determination for that Individual.
21. "Insurance Affordability Programs" means (1) APTCs or CSRs; (2) a State Medicaid program under title XIX of the Social Security Act; (3) a State children's health insurance program (CHIP) under title XXI of the Social Security Act; and (4) a State program under section 1331 of the ACA establishing qualified basic health plans.
22. "Medicaid" means the health benefit program established under Title XIX of the Social Security Act.
23. "Minimum Essential Coverage" or "MEC" has the meaning given in § 5000A(f) of the Internal Revenue Code of 1986, 26 U.S.C. § 5000A, as enacted by § 1501 of the ACA. See 45 C.F.R. 155.320(b). Under final rules adopted by the Department of the Treasury, Internal Revenue Service to implement 26 U.S.C. § 5000A at 26 C.F.R. § 1.5000A-2, enrollment in Medicaid or CHIP only for the following limited benefit packages does not constitute minimum essential coverage because they do not necessarily provide a scope of benefits comparable to the Medicaid or CHIP coverage provided to categorically eligible individuals:
 - 1) Coverage limited to family planning services under § 1902(a)(10)(A)(ii)(XXI) of the Social Security Act (42 U.S.C. 1396a(a)(10)(A)(ii)(XXI));
 - 2) Coverage limited to tuberculosis-related services under § 1902(a)(10)(A)(ii)(XII) (42 U.S.C. 1396a(a)(10)(A)(ii)(XII));
 - 3) Coverage limited to pregnancy-related services for pregnant women eligible under § 1902(a)(10)(A)(i)(IV) and (a)(10)(A)(ii)(IX) (42 U.S.C. 1396a(a)(10)(A)(i)(IV), (a)(10)(A)(ii)(IX)), unless the coverage afforded under the state plan to such pregnant women consists of full Medicaid benefits equivalent to those provided to other categorically needy pregnant beneficiaries, per SHO #14-002;

- 4) Coverage provided to otherwise eligible non-qualified non-citizens, which is limited to treatment of emergency medical conditions under 8 U.S.C. 1611(b)(1)(A), as authorized by § 1903(v) of the Social Security Act (42 U.S.C. 1396b(v));
 - 5) Coverage provided to medically needy individuals who are required to meet a spend-down amount in order to establish medically needy eligibility, as authorized by §1902(f)(2) of the Social Security Act, unless recognized as minimum essential coverage under §5000A(f)(1)(E) or eligible for coverage under the 209(b) category per §5000A(f)(1)(A)(ii) and the implementing IRS regulations;
 - 6) Coverage provided through Designated State Health Programs (DSHP) as authorized under section 1115, unless the state has obtained a designation of minimum essential coverage from the HHS Secretary in accordance with regulations at 45 CFR 156.604;
 - 7) Coverage provided through Section 1115 demonstration projects that do not provide the same benefits and coverage as that afforded to mandatory categorically needy individuals eligible under the state plan, as determined by the HHS Secretary;
 - 8) Coverage limited to a specific category of benefits such as prescription drugs, services to treat a specific medical condition, or services available from a limited, local network of providers which does not meet the minimum essential coverage standard;
 - 9) Coverage under the option to cover unborn children as targeted low-income children under CHIP, as set forth in 42 CFR 257.10.
24. "PII" means personally identifiable information as defined by OMB Memorandum M-07-16 (May 22, 2007). "PII refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."
25. "Protected Health Information" (or "PHI") has the same meaning as provided in the definition of "Protected Health Information" in the HIPAA Privacy Rule at 45 CFR § 160.103.
26. "QHP" (qualified health plan) means a health plan that has in effect a certification that it meets the standards described in 45 C.F.R. part 156, subpart C issued or recognized by each Exchange through which such plan is offered in accordance with the process described in 45 C.F.R. part 155, subpart K.
27. "Record" is defined in the Privacy Act at 5 U.S.C. § 552a(a)(4) as any item, collection, or grouping of information about an individual that is maintained by an agency, including,

but not limited to, his or her education, financial transactions, medical history, and criminal or employment history and that contains his or her name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

28. “Redetermination” means the process by which an Exchange determines eligibility for a qualified Individual or Enrollee in one of two circumstances: (1) on an annual basis prior during open enrollment; and/or (2) when an Individual communicates an update to an Exchange that indicates a change to the Individual’s circumstances affecting his or her eligibility.
29. “Renewal” means the annual process for an Enrollee to be considered for continued coverage under a State Medicaid program or a Children’s Health Insurance Program (CHIP).
30. “Return Information” is as defined under 26 U.S.C. §6103(b)(2) and has the same meaning as Federal Tax Information (FTI) as used in IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies.
31. “SBE” means a State-based Exchange, which is an Exchange established by a state under § 1311(b) that is subject to the requirements at 45 C.F.R. §§ 155.10 – 155.1405.
32. “SBE-FP” means a State-based Exchange on the Federal platform, which is an Exchange established by a state under § 1311(b) that meets certain obligations, including eligibility determinations for APTC and enrollment in QHP coverage, by relying on Federal services that the Federal government agrees to provide under a Federal platform agreement, as provided under 45 C.F.R. § 155.200(f).
33. “SSR” means “Safeguard Security Report” required by 26 U.S.C. § 6103(p)(4)(E) and filed in accordance with IRS Publication 1075 to detail the safeguards established to maintain the confidentiality of Return Information received from the Hub or in an account transfer.
34. “System of Records” means the same as that term defined in the Privacy Act at 5 U.S.C. § 552a(a)(5). It is a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

V. PROGRAMS AND DATA EXCHANGE SYSTEMS

A. Records Description

1. Minimum Essential Coverage Verification

Exchanges must request information from Medicaid and CHIP agencies to verify whether an Applicant or Enrollee has already been determined eligible for such programs. CMS

can request information through the Hub from Medicaid and CHIP agencies in states with an FFE or SBE-FP in accordance with 45 C.F.R. § 155.345 and 42 C.F.R. §§ 435.945 and 457.380(a)-(j) in order to verify an Applicant or Enrollee's eligibility or enrollment in the Medicaid/CHIP program.

Medicaid/CHIP agencies operating in states with an FFE or SBE-FP will respond to requests from the Hub to verify an Applicant or Enrollee's eligibility for or enrollment in the Medicaid/CHIP program. *See* 42 C.F.R. §§ 435.945(c) and 457.348.

The following descriptions of data elements to be exchanged apply only to Medicaid/CHIP agencies operating in states with an FFE or SBE-FP where the Medicaid/CHIP agency provides verification of an Applicant or Enrollee's eligibility or enrollment in the Medicaid/CHIP program to CMS in making an Eligibility Determination:

- a. From CMS to Medicaid/CHIP agency. For each Applicant or Enrollee seeking an Eligibility Determination at the FFE or an SBE-FP and on a quarterly basis thereafter, CMS will submit a request through the Hub to the Medicaid/CHIP agency in the state where the Individual resides that may include, but is not limited to, the following specified data elements:
 - i. Social Security Number (if applicable)
 - ii. Last Name
 - iii. First Name
 - iv. Date of Birth
- b. From Medicaid/CHIP agency to CMS. The state Medicaid/CHIP agency will respond to CMS through the Hub on each request described above in Section V.A.1.a. The response may include, but is not limited to, the following specified data elements:
 - i. Minimum Essential Coverage (MEC) verification code
 - ii. MEC eligibility start date
 - iii. MEC eligibility end date

2. Account Transfers

CMS will develop procedures through which an electronic Account containing all of the Records and information about an Individual, will be transferred from the Medicaid/CHIP agency in states with an FFE or SBE-FP, through the Hub, to CMS once the Individual is determined by a state Medicaid/CHIP agency to be potentially eligible for an Insurance Affordability Programs other than Medicaid or CHIP. CMS will likewise develop procedures through which the Individual's Account for an Individual determined or assessed by CMS as eligible for Medicaid or CHIP will be transferred from CMS, through the Hub, to the Medicaid/CHIP agency or its designee in states with an FFE or SBE-FP.

The following descriptions of data elements to be exchanged apply only to a Medicaid/CHIP agency in a state with an FFE or SBE-FP and for purposes of Account Transfers:

a. From CMS to Medicaid/CHIP agency.

- i. For each Applicant or Enrollee determined or assessed as eligible for Medicaid or CHIP by CMS, CMS will engage in an Account Transfer of authorized information pursuant to 45 C.F.R. §§ 155.302 and/or 155.345. Return Information in an Individual's Account may only be transferred to Medicaid or CHIP agencies with an IRS approved Safeguard Procedures Report (SPT).
- ii. For Account Transfers made from CMS to the Medicaid/CHIP agency for individuals for whom another insurance affordability program has not made a determination of Medicaid eligibility, but who have been assessed by such program (including as a result of a decision made by the Exchange appeals entity) as potentially Medicaid eligible, and for individuals not so assessed, but who otherwise request a full determination by the Medicaid agency, the Medicaid/CHIP agency must notify CMS, through the Hub, of the final Eligibility Determination of the Applicant or Enrollee for Medicaid or CHIP, pursuant to 42 C.F.R. §§ 435.1200(d)(5) and 457.348(c)(6).

b. From Medicaid/CHIP agency to CMS

- i. For each Applicant or Enrollee assessed as potentially eligible for other Insurance Affordability Programs, the Medicaid/CHIP agency will engage in an Account Transfer of authorized information pursuant to 42 C.F.R. §§ 435.1200(e)(i) and 457.350(i) and 45 C.F.R. §§ 155.302 or 155.345.

VI. RETENTION AND DISPOSITION OF IDENTIFIABLE RECORDS

Medicaid/CHIP agencies and CMS will retain all identifiable records in accordance with applicable law.

VII. SAFEGUARDS AND INCIDENT REPORTING

A. Safeguards

1. The Medicaid and CHIP agency shall comply with all applicable regulations regarding the privacy and security of PII, including provisions of the HIPAA Privacy and Security Rules at 45 C.F.R. Parts 160 and 164, that govern protections for individually identifiable health information (such as eligibility for health coverage under the Medicaid or CHIP program(s)).
2. The Medicaid/CHIP agency must comply with Minimum Acceptable Risk Standards for Exchanges (MARS-E), version 2.0 dated November 15, 2015 which includes the

following suite of documents: Volume I: Harmonized Security and Privacy Framework; Volume II: Minimum Acceptable Risk Standards for Exchanges; Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges; and Volume IV: ACA Administering Entity System Security Plan The version 2.0, November 15, 2015 MARS-E suite of documents may be found via this link: <https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/#MinimumAcceptableRiskStandards>.

3. For all PII under this Agreement, the Medicaid/CHIP agency must comply with the following privacy and security requirements and obligations:
 - a. An AE shall ensure that its employees, contractors, and agents implement the appropriate administrative, physical and technical safeguards to protect data furnished by CMS under this Agreement (including data which constitutes PII) from loss, theft or inadvertent disclosure.
 - i. Administrative Safeguards. Both Parties will advise all users who will have access to the data (including but not limited to any data derived from the exchange) of the confidential nature of the data, the safeguards required to protect the data, and the civil and criminal sanctions for noncompliance contained in applicable Federal laws.
 - ii. Physical Security/Storage: Both Parties will store the data and any data derived from the exchange in an area that is physically and technologically secure from access by unauthorized persons during duty hours, as well as non-duty hours or when not in use (e.g., door locks, card keys, biometric identifiers, etc.). Only authorized personnel will transport the data and any data derived from the exchange. Both Parties will establish appropriate safeguards for such data, as determined by a risk-based assessment of the circumstances involved.
 - iii. Technical Safeguards: Both Parties agree that the data exchanged under this Agreement 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. AE personnel must enter personal identification numbers when accessing data on the Party's systems. Both Parties will strictly limit authorization to those electronic data areas necessary for authorized persons to perform his or her official duties.

- iv. Understand that they are responsible for safeguarding this information at all times, regardless of whether or not the AE employee, contractor, or agent is at his or her regular duty station.
- v. Ensure that laptops and other electronic devices/media containing data that constitutes PII are encrypted and/or password protected.
- vi. Send E-mails containing data that constitutes PII only if encrypted and being sent to and received by email addresses of persons authorized to receive such information. In the case of FTI, AE employees, contractors, and agents must comply with IRS Publication 1075's rules and restrictions on emailing return information.
- vii. Restricted access to the data only those authorized AE employees, contractors, and agents who need such data to perform their official duties in connection with purposes identified in this Agreement; such restrictions shall include, at a minimum, role-based access that limits access to those individuals who need it to perform their official duties in connection with the uses of data authorized in this Agreement ("authorized users"). Further, the AE shall advise all users who will have access to the data provided under this Agreement and to any data derived from the data exchange contemplated by this Agreement of the confidential nature of the data, the safeguards required to protect the data, and the civil and criminal sanctions for noncompliance contained in the applicable Federal laws. The AE shall require its contractors, agents, and all employees of such contractors or agents with authorized access to the data disclosed under this Agreement, to comply with the terms and conditions set forth in this Agreement, and not to duplicate, disseminate, or disclose such data unless authorized under this Agreement.
- viii. For receipt of FTI, AE agree to maintain all return information sourced from the IRS in accordance with IRC section 6103(p)(4) and comply with the safeguards requirements set forth in 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 CFR 301.6103(p)(4)-1. In addition, IRS safeguarding requirements require all AE to which CMS provides return information to:
 - (1) Establish a central point of control for all requests for and receipt of Return Information, 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.

- (2) Establish procedures for secure storage of return information consistently maintaining two barriers of protection to prevent unauthorized access to the information, including when in transit, in accordance with Publication 1075.
- (3) Consistently label return information obtained under this Agreement to make it clearly identifiable and to restrict access by unauthorized individuals. Any duplication or transcription of return information creates new records which must also be properly accounted for and safeguarded. Return information should not be commingled with other Agency records unless the entire file is safeguarded in the same manner as required for return information and the FTI within is clearly labeled in accordance with Publication 1075.
- (4) Restrict access to return information solely to officers, employees, agents, and contractors of AE whose duties require access for the purposes of carrying out this Agreement. Prior to access, AE must evaluate which personnel require such access on a need-to-know basis. Authorized individuals may only access return information to the extent necessary to perform services related to this Agreement, in accordance with Publication 1075.
- (5) Prior to initial access to FTI and annually thereafter, AE will ensure that employees, officers agents, and contractors that will have access to return information receive awareness training regarding the confidentiality restrictions applicable to the return information and certify acknowledgement in writing that they are informed of the criminal penalties and civil liability provided by sections 7213, 7213A, and 7431 of the Code for any willful disclosure or inspection of return information that is not authorized by the Code, in accordance with Publication 1075.
- (6) Prior to initial receipt of return information, have an IRS approved Safeguard Security Report (SSR). Each AE must annually thereafter submit an SSR. Each Administering Entity's Head of Agency must certify the SSR fully describes the procedures established for ensuring the confidentiality of return information, addresses all outstanding actions identified by the Office of Safeguards from a prior year's SSR submission; 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 the FTI in accordance with Publication 1075 and the commitment to assist the Office of Safeguards in the joint effort of protecting the confidentiality of FTI; report all data incidents involving return information to the Office of Safeguards and Treasury Inspector General for Tax Administration (TIGTA) timely and to cooperate with TIGTA and Office of Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the incident; support the Office of Safeguards' on-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 (IT) divisions to secure pre-approval, if needed, for automated system scanning and to support timely mitigation of identified risk to return information in a Corrective Action Plan (CAP) for as long as return information is received or retained. SSRs will be transmitted in electronic format and on the template provided by Office of Safeguards using an IRS-approved encryption method in accordance with Publication 1075.

- (7) Ensure that Return Information is properly destroyed or returned to the IRS when no longer needed based on established AE record retention schedules in accordance with Publication 1075, or after such longer time required by applicable law.
- (8) Conduct periodic internal inspections of facilities where Return Information is maintained to ensure IRS safeguarding requirements are met and will permit the IRS access to such facilities as needed to review the extent to which AE is complying with the requirements of this section.
- (9) Each Administering Entity must ensure information systems processing return information are compliant with Section 3544(a)(1)(A)(ii) of the Federal Information Security Management Act of 2002 (FISMA). Each Administering Entity will maintain an SSR which fully describes the systems and security controls established at the 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 federal tax returns and return information are provided in Publication 1075.

- (10) Each Administering Entity agrees to report suspected unauthorized inspection or disclosure of return information within 24 hours of discovery to the appropriate Agent-in-Charge, Treasury Inspector General for Tax Administration (TIGTA), and to the IRS Office of Safeguards in accordance with as specified in Publication 1075.
- (11) CMS must ensure that contracts with contractors and subcontractors performing work involving return information under this agreement contain specific language requiring compliance with IRC section 6103(p)(4) and Publication 1075 safeguard requirements and enforces CMS' right to, and permits IRS access to, contractor and subcontractor facilities to conduct periodic internal inspections where return information is maintained to ensure IRS safeguarding requirements are met.
- (12) Officers, employees and agents who inspect or disclose Return Information obtained pursuant to this Agreement in a manner or for a purpose not so 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 AE could be required to defend a civil damages action under section 7431.
- (13) IRS will conduct periodic safeguard reviews of the AE to assess whether security and confidentiality of Return Information is maintained consistent with the safeguarding protocols described in Publication 1075. Periodic safeguard reviews will involve the inspection of AE facilities and contractor facilities where FTI is maintained; the testing of technical controls for computer systems storing, processing or transmitting FTI; review of AE recordkeeping and policies and interviews of AE employees and contractor employees as needed, to verify the use of FTI and assess the adequacy of procedures established to protect FTI.
- (14) Recognize and treat all IRS Safeguards documents and related communications as IRS official agency records; that they are property of the IRS; that IRS records are subject to disclosure restrictions under Federal law and IRS rules and regulations and may not be released publicly under state Sunshine or Information Sharing/Open Records provisions

and that any requestor seeking access to IRS records should be referred to the Federal Freedom of Information Act (FOIA) statute. If the AE determines that it is appropriate to share Safeguards documents and related communications with another governmental function/branch for the purposes of operational accountability or to further facilitate protection of FTI that the recipient governmental function/branch must be made aware, in unambiguous terms, that Safeguards documents and related communications are property of the IRS; 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 safeguards documents must forward them to IRS for reply.

4. The Medicaid/CHIP agency shall ensure that their employees, contractors, and agents:
 - a. Implement administrative, physical and technical safeguards to protect PII furnished by CMS under this Agreement from loss, theft or inadvertent disclosure;
 - b. Understand that they are responsible for safeguarding this information at all times, regardless of whether or not the Medicaid/CHIP agency employee, contractor, or agent is at his or her regular duty station;
 - c. Ensure that laptops and other electronic devices/media containing PII are encrypted and/or password protected;
 - d. Send emails containing PII only if encrypted and being sent to and being received by email addresses of persons authorized to receive such information; and
 - e. Limit disclosure of the information and details relating to a PII loss only to those who need to know the information to carry out authorized functions under this Agreement or to address the PII loss in accordance with applicable law.
5. The Medicaid/CHIP agency shall restrict access to the data obtained under this Agreement to only those authorized Medicaid/CHIP agency employees, contractors, and agents who need such data to perform their official duties in connection with purposes identified in this Agreement; such restrictions shall include, at a minimum, role-based access that limits access to those individuals who need it to perform their official duties in connection with the uses of data authorized in this Agreement ("authorized users"). Further, the Medicaid/CHIP agency shall advise all users who will have access to the data provided under this Agreement of the confidential nature of the data, the safeguards required to protect the data, and the civil and criminal sanctions for noncompliance contained in the applicable law. The Medicaid/CHIP agency shall require its contractors, agents, and all employees of such contractors or agents with authorized access to the data disclosed under this Agreement, to comply

with the terms and conditions set forth in this Agreement, and to bind such contractors or agents not to duplicate, disseminate, or disclose such data without the MSA/CHIP program, obtaining prior written approval from CMS.

B. For Return Information, the Medicaid/CHIP agency attest that it will:

1. Comply with the standards and protocols in 45 C.F.R. § 155.260(b)(3)-(8), which provides that Return Information, as defined in § 6103(b)(2) of the Internal Revenue Code, must be kept confidential and collected, used, disclosed, and maintained in accordance with § 6103 of the Internal Revenue Code, and 1942(b) of the Social Security Act.
2. Not retain any Return Information longer than necessary to conduct the minimum functions related to eligibility or Exemption determinations, appeals, and submission of notices unless required to do so by law. While maintained, CMS and Medicaid/CHIP agencies will maintain all Return Information received in an Individual account transfer in accordance with 26 U.S.C. § 6103(p)(4) and also comply with all additional Federal safeguards required by IRS Publication 1075.
3. Not create a separate file or system of records consisting of information concerning only those individuals who are involved in Agreement, except as is necessary to control or verify the information for purposes of this program or to operate program.
4. Establish a central point of control for all requests for and receipt of Return Information, 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.
5. Establish procedures for secure storage of Return Information consistently maintaining two barriers of protection to prevent unauthorized access to Return Information, including when in transit, in accordance with Publication 1075.
6. Consistently label Return Information obtained under this Agreement to make it clearly identifiable and to prevent access by unauthorized individuals. Any duplication or transcription of Return Information creates new records which must also be properly accounted for and safeguarded. Return Information should not be commingled with other records unless the entire file is safeguarded in the same manner as required for Return Information and the Return Information within is clearly identified (i.e. labeled).
7. Restrict access to Return Information solely to officers, employees and contractors of CMS whose duties require access for the purposes of carrying out this agreement. Prior to access, Agency must evaluate which employees require such access. Authorized individuals may only access Return Information to the extent necessary to

perform services related to this agreement, in accordance with Publication 1075.

8. Prior to initial access to Return Information and annually thereafter, Agency will ensure that employees, officers, and contractors that will have access to Return Information receive awareness training regarding the confidentiality restrictions applicable to Return Information and certify acknowledgement in writing that they are informed of the criminal penalties and civil liability provided by IRC Sections 7213, 7213A, and 7431 for any willful disclosure or inspection of Return Information not authorized by the IRC, in accordance with Publication 1075.
9. Prior to initial receipt of Return Information, Agency must have an IRS approved SSR. Agency must annually thereafter submit an SSR to the IRS Safeguards by the submission deadline specified in Publication 1075. Head of Agency must certify the SSR fully describes the procedures established for ensuring the confidentiality of Return Information, addresses all Outstanding Actions identified by the IRS Safeguards from a prior year's SSR submission; accurately and completely reflects the current physical and logical environment for the receipt, storage, processing and transmission of Return Information; accurately reflects the security controls in place to protect the Return Information in accordance with Publication 1075 and the commitment to assist the IRS Safeguards in the joint effort of protecting the confidentiality of Return Information; report all data incidents involving Return Information to the IRS Safeguards and TIGTA timely and to cooperate with TIGTA and IRS Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the incident; support the IRS Safeguards' on-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 (IT) divisions to secure pre-approval, if needed, for automated system scanning and to support timely mitigation of identified risk to Return Information in a Corrective Action Plan (CAP) for as long as Return Information is received or retained. SSRs will be transmitted in electronic format and on the template provided by IRS Safeguards using an IRS-approved encryption method in accordance with Publication 1075.
10. Agency will ensure that Return Information is properly destroyed or returned to the IRS when no longer needed in accordance with Publication 1075.
11. Agency will conduct periodic internal inspections of facilities where Return Information is maintained to ensure IRS safeguarding requirements are met and will permit the IRS access to such facilities as needed to review the extent to which Agency is complying with the IRC Section 6103(p)(4) requirements of this section.
12. Ensure information systems processing Return Information are compliant with § 3544(a)(1)(A)(ii) of the Federal Information Security Management Act of 2002 (FISMA). Agency will maintain an SSR which fully describes the systems and security controls established at the 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 federal tax returns and Return Information are provided in Publication 1075.

C. Incident Reporting

1. The Medicaid/CHIP agency shall handle and report to CMS Incidents in accordance with the organization's documented Incident Handling and Breach Notification procedures in accordance with 42 C.F.R. §§ 431.300- 431.306 and 435.945. Medicaid/CHIP agency procedures should address how the Medicaid or CHIP agency will:
 - a. Identify Incidents;
 - b. Determine if personally identifiable information is involved in Incidents;
 - c. Report suspected or confirmed Incidents;
 - d. Identify and convene a core response group within the Medicaid/CHIP agency to determine the risk level of Incidents and determine risk-based responses to Incidents;
 - e. Determine whether Breach notification is required, and, if so, identify appropriate Breach notification methods, timing, source, and contents from among different options, and bear costs associated with the Breach notice as well as any mitigation measures; and
 - f. Disclose information about individuals whose information may have been compromised, misused, or changed without proper authorization, and the persons who disclosed the PII improperly, to federal, state, or local law enforcement investigators in connection with efforts to investigate and mitigate the consequences of any Incidents as authorized by federal, state, or local law.
2. When conducting functions under this agreement, the Medicaid/CHIP agency shall report any suspected or confirmed Incidents affecting loss or suspected loss of PII within one hour of discovery to their designated CCIIO State Officer who will then notify the affected federal agency data sources, i.e., Internal Revenue Service, Department of Defense, Department of Homeland Security, Social Security Administration, Peace Corps, Office of Personnel Management or Veterans Health Administration. Additionally, the Medicaid/CHIP agency shall contact the office of the appropriate Special Agent-in-Charge, Treasury Inspector General for Tax Administration (TIGTA), and the IRS Office of Safeguards within 24 hours of discovery of any potential breach, loss, or misuse of Federal Tax Information. Contact information is contained in IRS Publication 1075.
3. When conducting functions under this agreement the Medicaid/CHIP agency shall;
 - a. Email the CMS IT Service Desk at cms_it_service_desk@cms.hhs.gov within one hour of discovery of incidents (including incidents involve Federal Tax Information (FTI)*):
 - b. If unable to report incidents to the CMS IT Service Desk via email, contact the CMS IT Service Desk by phone at (800) 562-1963 or (410) 786-2580.
 - c. Complete and submit the CMS ACA Security and Privacy Incident Reporting Template (doc88794) to the CMS IT Service Desk for all reported incidents.

- d. Submit electronic after-action reports to CMS Information Systems Security Officers (ISSOs) after incidents are resolved.
4. ***If Incidents involve FEDERAL TAX INFORMATION (FTI): Return Information**
1. Contact the U.S. Treasury Inspector General for Tax Administration (TIGTA) and the IRS Office of Safeguards (OTS) immediately, but no later than 24 hours after identification of a possible issue involving FTI. In addition, contact the CMS IT Service Desk within one hour of incident discovery following guidance in the aforementioned paragraphs.
- TIGTA Hotline number: 1-800-589-3718
 - Website: U.S. Treasury Inspector General for Tax Administration (TIGTA)
 - IRS Office of Safeguards: safeguardreports@irs.gov

VIII. INTEGRATION CLAUSE

This Agreement constitutes the entire agreement of the Parties with respect to its specific subject matter and supersedes all other data exchange agreements between the Parties that pertain to the disclosure and transmission of the data specifically described herein between CMS and Medicaid/CHIP agencies for the specific purposes described in this Agreement. Neither Party has made representations, warranties, or promises outside of this Agreement. This Agreement takes precedence over any prior documents that may be in conflict with it, and any subsequent documents that do not expressly supersede it.

IX. SEVERABILITY

If any term or other provision of this Agreement is determined to be invalid, illegal or incapable of being enforced by any rule or law, or public policy, all other terms, conditions, or provisions of this Agreement shall nevertheless remain in full force and effect, provided that the data exchange program contemplated hereby would not be affected in any manner materially adverse to any Party. Upon such determination that any term or other provision is invalid, illegal or incapable of being enforced, the Parties hereto shall negotiate in good faith to modify this Agreement so as to effect the original intent of the Parties as closely as possible, in an acceptable manner to both Parties, to the end that the transactions contemplated by this Agreement are executed to the fullest extent possible.

X. CMS POINTS OF CONTACT

A. CMS – Exchange contact for Programmatic issues:

Jenny Chen, MPH

Director, State Technical Assistance Division
State Marketplace and Insurance Programs Group (SMIPG)
Center for Consumer Information and Insurance Oversight
Centers for Medicare & Medicaid Services
7501 Wisconsin Avenue, Bethesda, MD 20814
Telephone: 301-492-5156
E-mail: Jenny.Chen@cms.hhs.gov

Robert Yates

State Operations Division
State Marketplace and Insurance Programs Group (SMIPG)
Center for Consumer Information and Insurance Oversight
Centers for Medicare & Medicaid Services
7501 Wisconsin Avenue, Bethesda, MD 20814
Telephone: 301-492-5151
E-mail: Robert.Yates@cms.hhs.gov

B. CMS – Medicaid/CHIP contact for Programmatic issues:

Sarah L. Spector

Deputy Director
Division of Eligibility, Enrollment and Outreach
Center for Medicaid and CHIP Services
Centers for Medicaid & Medicare Services
7500 Security Boulevard
Mail Stop: S2-01-16
Location: S2-07-03
Baltimore, MD 21244-1850
Telephone: (410) 786-3031
Email: Sarah.spector@cms.hhs.gov

C. CMS contact for Privacy Policy issues:

Walter Stone

CMS Privacy Act Officer
Division of Security, Privacy Policy and Governance
Information Security and Privacy Group
Office of Information Technology
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Location: N1-14-56
Baltimore, MD 21244-1850
Telephone: (410)786-5357

E-mail: walter.stone@cms.hhs.gov

Barbara Demopulos, CMS Privacy Advisor

Division of Security, Privacy Policy and Governance

Information Security and Privacy Group

Office of Information Technology

Centers for Medicare & Medicaid Services

7500 Security Boulevard

Location: N1-14-40

Baltimore, MD 21244-1850

Telephone: (410) 786-6340

E-mail: Barbara.Demopulos@cms.hhs.gov

Scott Blumberg, Privacy Advisor

Division of Security, Privacy Policy & Governance

Information Security & Privacy Group

Office of Information Technology

Centers for Medicare & Medicaid Services

Location: N1-15-25

7500 Security Boulevard

Baltimore, MD 21244-1850

Telephone: (410) 786-7329

E-mail: Scott.Blumberg@cms.hhs.gov

XI. EFFECTIVE DATE, TERM, MODIFICATION, AND TERMINATION

A. Effective Date, Term and Renewal

The effective date of this Agreement is October 2, 2019 and this Agreement will remain valid for a period of 5 years. This Agreement may be renewed for consecutive 5 year periods, subject to the requirements of the Parties. If either Party does not want to extend this Agreement, it should notify the other in writing at least ninety (90) days prior to the expiration of this Agreement.

B. Modification

The Parties may modify this Agreement at any time by executing a written modification, mutually agreed upon by both Parties.

C. Termination

This Agreement may be terminated at any time upon the mutual written consent of the Parties.

D. Survival

The Parties' privacy, security, document retention, document destruction, and incident response duties under sections VI and VII of this Agreement shall survive termination of this Agreement.

XII. APPROVALS

A. Centers for Medicare & Medicaid Services Program Official

The authorized program official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits his respective organization to the terms of this Agreement.

Approved By (Signature of Authorized CMS Program Official)	
Jeffrey Grant -S Digitally signed by Jeffrey Grant -S Date: 2019.09.19 17:06:25 -04'00'	
Jeffrey D. Grant Deputy Director for Operations Center for Consumer Information and Insurance Oversight Centers for Medicare & Medicaid Services	Date:

B. Centers for Medicare & Medicaid Services Privacy Official

The authorized privacy official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits his respective organization to the terms of this Agreement.

Approved By (Signature of Authorized CMS Privacy Official)

Michael E. Pagels -S_{Digitally signed by Michael E. Pagels -S}
Date: 2019.09.20 10:33:44 -04'00'

**Michael Pagels, Director
Division of Security, Privacy Policy and Governance, and
Acting Senior Official for Privacy
Information Security Privacy Group
Office of Information Technology
Centers for Medicare & Medicaid Services**

Date:

C. Centers for Medicare & Medicaid Services Approving Official

The authorized approving official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits his/her respective organization to the terms of this Agreement.

Approved By (Signature of Authorized CMS Approving Official)


Karen M. Shields -S Digitally signed by Karen M. Shields -S
Date: 2019.09.27 09:47:46 -04'00'

Karen Shields
Deputy Director
Centers for Medicaid and CHIP Services
Centers for Medicare & Medicaid Services

Date:

D. State-Based Exchange Program Official

The authorized State-Based Exchange program official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits his/her respective organization to the terms of this Agreement.

Approved by (Signature of Authorized State-Based Exchange Official)	
	
Name: Shaunda O'Brien Title: Director Organization: Division of Public Assistance	Date: 10.4.19