INFORMATION EXCHANGE AGREEMENT
BETWEEN
THE CENTERS FOR MEDICARE & MEDICAID SERVICES
AND
THE DEPARTMENT OF HOMELAND SECURITY
U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
FOR DISCLOSURE OF
IDENTITY AND LOCATION INFORMATION OF ALIENS

CMS Information Exchange Agreement No. 2025-80

Effective Date: July 9, 2025
Expiration Date: September 9, 2025

I. PURPOSE

This Information Exchange Agreement, hereinafter the "Agreement," establishes the conditions, safeguards, and procedures that govern the exchange of data between the Centers for Medicare & Medicaid Services (CMS) and the Department of Homeland Security (DHS) U.S. Immigration and Customs Enforcement (ICE), hereinafter, each referred to as a "Party" and collectively "the Parties." ICE will be provided access to the CMS Integrated Data Repository to retrieve information concerning the identity and location of aliens in the United States.

Access to this information will allow ICE to receive information concerning the identity and location of aliens in the United States, such as address, telephone number, banking information (routing number, account type, account number), email address, internet protocol (IP) addresses, or other information relevant to identifying and locating aliens in the United States. By entering into this Agreement, the Parties agree to comply with the terms and conditions set forth herein, as well as applicable law and regulations. The terms and conditions of this Agreement will be carried out by authorized officers, employees, and contractors of CMS and ICE.

Any disclosure(s) of CMS Data, or any individually identifiable derivative of this CMS Data, by the undersigned or its agents to a Downstream User, as defined below, shall be made in accordance with applicable law as well as any applicable provisions in this or other governing documents.

The terms and conditions of this Agreement will be carried out by authorized officers, employees, and contractors of CMS and ICE.

CMS will serve as the source agency for this Agreement and ICE will serve as the recipient under this Agreement.

II. LEGAL AUTHORITIES

Among other potential provisions, the following statutes and regulations govern the exchange and/or disclosure of data under this Agreement:

The following authorities, including the Privacy Act, govern the program and disclosure of data under this Agreement:

A. This Agreement is executed in compliance with the Privacy Act of 1974, as amended (5 U.S.C. § 552a(b)(3)), section 1106 of the Social Security Act (42 U.S.C. § 1306) and the regulations and guidance promulgated thereunder.

B. Section 102 of the Homeland Security Act of 2002 (HSA), 6 U.S.C. § 112, and section 103 of the Immigration and Nationality Act (INA), 8 U.S.C. § 1103, vest the Secretary of Homeland Security with administration of the immigration and naturalization laws of the United States and the authority to enter into agreements with other executive agencies, as may be necessary and proper to carry out the Secretary's responsibilities.

C. Executive Order 14159 "Protecting the American People Against Invasion" issued on January 20, 2025, directs the Secretary of Homeland Security to take appropriate action to use all provisions of the immigration laws or any other Federal law to ensure the efficient and expedited removal of aliens from the United States. 90 Fed. Reg. 8443 (Jan. 29, 2025).

D. Section 202(a)(2) of the HSA, 6 U.S.C. § 122, provides that the Secretary of Homeland Security shall have access to information relating to matters under the responsibility of the Secretary that may be collected, possessed, or prepared by an agency of the Federal Government as the President may further provide. Pursuant to this statute, the Secretary may obtain material upon request and enter into cooperative agreements with other agencies to provide DHS officials with access to the data on a regular or routine basis, including requests or arrangements involving broad categories of material, access to electronic databases, or both.

E. Section 290(b) of the INA, 8 U.S.C. §1360(b), provides that any information in any records kept by any department or agency of the Government as to the identity and location of aliens in the United States shall be made available to DHS upon request made by the Secretary of Homeland Security to the head of any such department or agency.

F. Title 8 U.S.C. § 1373(a), provides that notwithstanding any other provision of Federal, State, or local law, a Federal, State, or local government entity or official may not prohibit or in any way restrict any government entity or official from sending to DHS information regarding the citizenship or immigration status, lawful or unlawful, of any individual.

G. Social Security Act §§ 1116(d)–(e), 1903(d), and 1904, 42 U.S.C. §§ 1316(d)–(e), 1396b(d), 1396c, authorize the Secretary of Health and Human Services (HHS), through the Centers for Medicare & Medicaid Services (CMS), to conduct periodic

reviews of state Medicaid plans and operations to determine compliance with federal requirements. These provisions permit the Secretary to withhold federal financial participation (FFP) if a state is found to be noncompliant, and to recover overpayments resulting from unallowable claims. The statute ensures that states are afforded due process protections, including formal notice and the opportunity for a hearing, prior to the imposition of any such sanctions.

H. 42 C.F.R. Part 430, Subpart C implements the enforcement authorities granted under the Social Security Act by establishing regulatory procedures for compliance determinations, disallowances, and withholding of FFP. This subpart details the steps CMS must follow when initiating a finding of noncompliance, including the issuance of a formal notice to the state, the state's right to request an administrative hearing, and the criteria under which CMS may proceed with corrective or enforcement actions. The regulation provides a transparent administrative process to ensure program integrity and federal oversight in the administration of state Medicaid programs.

This Agreement does not constitute a computer matching program as described in the Privacy Act, 5 U.S.C. § 552a(a)(8). This Agreement complies with the Privacy Act of 1974, as amended, and the regulations and guidance promulgated thereunder. Although this information exchange is not covered by the provisions of the Privacy Act that relate to computer matching, this Agreement does follow applicable requirements and other relevant provisions of the Privacy Act.

III. DEFINITIONS

The following definitions are applicable to this Agreement:

A. "Breach" means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information, or (2) an authorized user accesses, or potentially accesses personally identifiable information for an other than authorized purpose. OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017)

B. "CMS" means the Centers for Medicare & Medicaid Services. CMS regulatory authority includes the oversight of the Medicare program, the federal portion of the Medicaid program and State Children's Health Insurance Program, the Health Insurance Marketplace, and related quality assurance activities.

C. "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.

D. "Personally Identifiable Information" or "PII" is defined in OMB Memorandum M-17-

12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017), and refers to information which can be used to distinguish or trace an individual's identity, either alone or when combined with information that is linked or linkable to a specific individual.

E. "System of Records" or "SOR" is defined by the Privacy Act of 1974 at 5 U.S.C. § 552a(a)(5) and means 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.

IV. RESPONSIBILITIES OF THE PARTIES

A. CMS's Responsibilities:
   1. CMS will provide direct access to the T-MSIS to a select set of ICE employees via CMS login credentials.

B. ICE's Responsibilities:
   1. ICE employees will access the CMS T-MSIS after receiving their CMS Login Credentials. To receive credentials, users must:
      a. Apply for CMS Enterprise User Administration (EUA) ID
      b. Complete Information System Security and Privacy Awareness training
      c. Sign the HHS/CMS Rules of Behavior for Use of Information & IT Resources.
   2. ICE employees will access the T-MSIS to receive information concerning the identification and location of aliens in the United States.

V. DESCRIPTION OF THE DATA THAT MAY BE DISCLOSED

A. CMS will provide CMS Data from the following SOR: "Transformed-Medicaid Statistical Information System (T-MSIS)". System No. 09-70-0541; last modified at 84 FR 2230 (2/16/19). In addition to the aforementioned DHS authorities, data maintained in the T-MSIS will be released pursuant to Routine Use number 2 of the T-MSIS SOR Notification, which is to assist another Federal or state agency, agency of a state government, an agency established by state law, or its fiscal agent.

B. Number of Records and Frequency
ICE will have direct access via the Integrated Data Repository to the records for a period of two (2) months. During those two (2) months, CMS technical support will be available Monday-Friday 9:00 a.m. to 5:00 p.m. Eastern Daylight Time.

C. Data Elements
   1. Medicaid recipients: Name, address, assigned Medicaid identification number, social security number (SSN), date of birth, sex, phone number, locality, ethnicity and race.

VI. SECURITY PROCEDURES

ICE and CMS will comply with the requirements of the Federal Information Security Management Act (FISMA), 44 U.S.C. Chapter 35, as amended by the Federal Information Security Modernization Act of 2014 (Pub. L. 113-283); related Office of Management and Budget (OMB) circulars and memoranda; National Institute of Standards and Technology (NIST) directives; and the Federal Acquisition Regulations; and including any applicable amendments published after the effective date of this Agreement. These laws, directives, and regulations include requirements for safeguarding Federal information and information systems and personally identifiable information (PII) used in Federal agency business processes, as well as related reporting requirements. Both agencies recognize and implement the laws, regulations, NIST standards, and OMB directives, including those published subsequent to the effective date of this Agreement.

FISMA requirements apply to all Federal contractors, organizations, or entities that possess or use Federal information, or that operate, use, or have access to Federal information systems on behalf of an agency. Both agencies are responsible for oversight and compliance of their contractors and agents.

A. Incident Reporting
If either Party experiences an incident involving the loss or breach of PII provided by either Party under the terms of this Agreement, they will follow the incident reporting guidelines issued by OMB. In the event of a reportable incident under OMB guidance involving PII, the agency experiencing the event is responsible for following its established procedures, including notification to the proper organizations (e.g., United States Computer Emergency Readiness Team). In addition, the agency experiencing the incident will, within one hour, notify CMS IT Service Desk at (410) 786-2580 or email CMS_IT_Service_Desk@cms.hhs.gov.

B. Breach Notification
The Parties will follow PII breach notification policies and related procedures as issued by OMB and other applicable legal, regulatory, and administrative authorities. If the agency that experienced the breach determines the risk of harm requires notification to affected individuals or other remedies, that agency will carry out these remedies without cost to the other agency.

C. Administrative Safeguards
The Parties will restrict access to the data exchanged and to any data created by the exchange to only those authorized employees and officials who need it to perform their official duties in connection with the uses of the data authorized in this Agreement. Further, the Parties will advise all personnel who have access to the data exchanged and to any data created by 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 the applicable Federal laws.

D. Physical Safeguards
The Parties will store the data exchanged and any data created by the exchange in an area that is physically and technologically secure from access by unauthorized persons at all

times. Only authorized personnel will transport the data exchanged, and any data created by the exchange. The Parties will establish appropriate safeguards for such data, as determined by a risk-based assessment of the circumstances involved.

E. Technical Safeguards
The Parties will process the data exchanged and any data created by the exchange under the immediate supervision and control of authorized personnel in a manner that will protect the confidentiality of the data, so that unauthorized persons cannot retrieve any data by computer, remote terminal, or other means. Systems personnel must enter personal identification numbers when accessing data on the agencies' systems. The Parties will strictly limit authorization to those electronic data areas necessary for the authorized analyst to perform his or her official duties.

F. Monitoring Compliance with Security Procedures
The Parties agree to make available to each other upon request system security evidence for the purpose of making risk-based decisions. Requests for this information may be made by either Party at any time throughout the duration or any extension of this Agreement.

In signing this Agreement ICE attests that the CMS Data subject to this Agreement will be protected as required by applicable law, including through the establishment of appropriate administrative technical and physical safeguards to protect the integrity, security, and confidentiality of the data, and to prevent unauthorized use or access to it.

VII. RECORDS USAGE AND REDISCLOSURE RESTRICTIONS

The Parties agree that the data involved in the exchange contemplated by this Agreement will be used and disclosed only as provided in this Agreement.

A. The Parties will use and disclose the data only for the purposes described in this Agreement or required by applicable law, unless the other Party consents to the use or disclosure. The Party requesting permission must specify the following in writing: (1) which data will be used or disclosed, (2) to whom the data will be disclosed, (3) the reasons justifying such use or disclosure, and (4) the intended use of the data.
B. The Parties will not use the data to extract information concerning individuals therein for any purpose not specified by this Agreement or applicable law.
C. ICE will use the CMS data to allow ICE to receive identity and location information on aliens identified by ICE.
D. ICE must specify in writing what records would be re-used or re-disclosed, by whom they would be re-used or to whom they would be re-disclosed, and the purpose of such re-use or re-disclosure. When further disclosure is required by law, ICE will notify and consult with CMS as soon as practicable and as permitted by law.

VIII. RETENTION AND DISPOSITION OF IDENTIFIABLE RECORDS

Information obtained under this Agreement will be retained only as long as necessary to carry out the purposes stated in this Agreement and in accordance with applicable law, regulation, and policy, and will be disposed of thereafter, in accordance with the applicable National Archives and Records Administration (NARA) General Records Schedule(s) or

NARA-approved agency-specific records retention schedule(s). If no applicable retention schedule exists, the records are retained indefinitely or until NARA approves a schedule(s). If a litigation hold is in place, the records are retained until no longer needed in the litigation and the hold is lifted.

IX. APPROVAL AND DURATION OF AGREEMENT

A. Effective Date and Duration: This Agreement will become effective on the date when both Parties have signed it and will remain in effect for a period not to exceed two (2) months from that date. This Agreement may be renewed for consecutive periods subject to the requirements of the Parties. Information exchange activities will continue without interruptions during agreement renewal procedurals.

B. Modification: The Parties may modify this Agreement at any time by a written modification agreed upon by both Parties, provided that the change is not significant. A significant change would require a new Agreement.

C. Termination: Either Party may unilaterally terminate this Agreement upon written notice to the other Party, in which case the termination shall be effective immediately after the date of that notice or at a later date specified in the notice.

D. Survival: Terms and conditions in this Agreement for Security Procedures, Records Usage and Redisclosure Restrictions, and Retention and Disposition of Identifiable Records shall survive the termination or expiration of this Agreement until all data associated with this agreement is returned or disposed of in accordance with the terms of this Agreement.

X. INTEGRATION CLAUSE

The agreement constitutes the entire agreement of the Parties with respect to its subject matter and supersedes all other agreements between the Parties that pertain to the disclosure of the specified CMS data to ICE for the purposes described in this agreement. ICE and CMS have made no representations, warranties, or promises outside of this agreement. This agreement takes precedence over any other documents that may be in conflict with it.

XI. FUNDING

This Agreement does not result in the transfer of funds or create a financial obligation between the Parties. Each Party agrees to fund its own cost of participating in this Agreement. No provision of this Agreement shall be interpreted to require obligation or payment of funds in violation of the Anti-Deficiency Act, 31 U.S.C. § 1341. All activities contemplated by this Agreement are subject to the availability of funds and other resources to the Parties.

XII. PERSONS TO CONTACT

Both Parties agree to designate key contacts and to keep the other informed of any changes to those contact persons.

1. CMS Contacts

Systems Issues:

Name: Keith Busby
Title: Acting Chief Information Security Officer
Organization: Office of Information Technology, Information Systems and Privacy Group
Telephone: 240-904-1113
Email: Keith.Busby@cms.hhs.gov

Name: Mark Hogle
Title: Group Director
Organization: Office of Information Technology, Enterprise Architecture & Data Group
Telephone: 410-786-6966
Email: Mark.Hogle@cms.hhs.gov

Agreement Coordination:

Name: Leslie Nettles
Title: Senior Official for Privacy
Organization: Office of Information Technology, Information Systems and Privacy Group
Telephone: 443-752-4322
Email: Leslie.Nettles1@cms.hhs.gov

2. Department of Homeland Security Contacts

Agreement Coordination:
Name: Mason Wilhite
Title: Special Assistant to the Deputy Assistant Director
Organization: U.S. Department of Homeland Security, Homeland Security Investigations (HSI), Cyber and Operational Technology
Telephone: 646-276-8530
Email: MASON.WILHITE@hsi.dhs.gov

XIII. SIGNATURES

A. Centers for Medicare & Medicaid Services Program Official Designee
The authorized program official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, and confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits their respective organization to the terms of this Agreement.

Electronic Signature Acknowledgement: The signatories may sign this document electronically by using an approved electronic signature process. Each signatory electronically signing this document agrees that his/her electronic signature has the same legal validity and effect as his/her handwritten signature on the document, and that it has the same meaning as his/her handwritten signature.

Approved by:

PATRICK I. NEWBOLD -S

Digitally signed by PATRICK I. NEWBOLD -S
Date: 2025.07.15 12:24:07 -04'00'

Patrick Newbold
Chief Information Officer
Director, Office of Information Technology
Centers for Medicare & Medicaid Services

B. 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, and confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits their respective organization to the terms of this Agreement.

Electronic Signature Acknowledgement: The signatories may sign this document electronically by using an approved electronic signature process. Each signatory electronically signing this document agrees that his/her electronic signature has the same legal validity and effect as his/her handwritten signature on the document, and that it has the same meaning as his/her handwritten signature.

Approved By:

Leslie Nettles -S Digitally signed by Leslie Nettles -S
Date: 2025.07.15 11:16:17 -04'00'

Leslie Nettles
Director, Division of Security, Privacy Policy and Oversight, and
Senior Official for Privacy
Information Security and Privacy Group
Office of Information Technology
Centers for Medicare & Medicaid Services

C. U.S. Immigration and Customs Enforcement Program Official

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

Electronic Signature Acknowledgement: The signatories may sign this document electronically by using an approved electronic signature process. Each signatory electronically signing this document agrees that his/her electronic signature has the same legal validity and effect as his/her handwritten signature on the document, and that it has the same meaning as his/her handwritten signature.

Approved by:

Marcos D. Charles
Acting Executive Associate Director
Enforcement and Removal Operations
U.S. Immigration and Customs Enforcement

Approved by:

07/10/2025

Derek W. Gordon
Acting Executive Associate Director
Homeland Security Investigations
U.S. Immigration and Customs Enforcement