



Billing Code: 4120-03

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Medicare & Medicaid Services

Privacy Act of 1974; System of Records

AGENCY: Centers for Medicare & Medicaid Services (CMS), Department of Health and Human Services (HHS).

ACTION: Notice of a Modified System of Records.

SUMMARY: The Department of Health and Human Services (HHS), Centers for Medicare & Medicaid Services (CMS), proposes to modify or alter an existing system of records subject to the Privacy Act, System No. 09-70-0541, titled “Medicaid Statistical Information System (MSIS).” This system of records covers the Medicaid dataset. The dataset includes standardized enrollment, eligibility, and paid claims of Medicaid recipients and is used to administer Medicaid at the Federal level, produce statistical reports, support Medicaid related research, and assist in the detection of fraud and abuse in the Medicare and Medicaid programs. CMS is adding two new routine use as numbers three and 10. CMS is including two routine uses that were published on February 14, 2018, and are numbered as eight and nine in the routine use section below. In addition, CMS is changing the name of the system of records to: Transformed-Medicaid Statistical Information System (T-MSIS) and making other modifications which are explained below.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this notice is applicable **[INSERT DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**, subject to a 30-day period in which to comment on the routine uses. Submit any comments by **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**.

ADDRESSES: Written comments should be submitted by mail or e-mail to: CMS Privacy Act Officer, Division of Security, Privacy Policy & Governance, Information Security & Privacy Group, Office of Information Technology, CMS, Location N1-14-56, 7500 Security Boulevard, Baltimore, MD 21244-1870, or walter.stone@cms.hhs.gov.

FOR FURTHER INFORMATION CONTACT: General questions about the system of records may be submitted to Darlene Anderson, Health Insurance Specialist, Data and Systems Group, Center for Medicaid and CHIP Services (CMCS), CMS, Mail Stop S2-22-16, 7500 Security Boulevard, Baltimore, MD 21244, Telephone 410-786- 9828 or e-mail to Darlene.Anderson@cms.hhs.gov.

SUPPLEMENTARY INFORMATION:

I. Program and IT System Changes Prompting this SORN Modification.

The Transformed Medicaid Statistical Information System (T-MSIS) is replacing the Medicaid Statistical Information System (MSIS) as the information technology (IT) system housing the national Medicaid dataset. It is a joint effort by the States and CMS to build a Medicaid dataset that addresses problems identified with Medicaid data in MSIS. T-MSIS provides improved program monitoring and oversight, technical assistance with states, policy implementation and data-driven and high-quality Medicaid program and Children's Health Insurance Program (CHIP) that ensure better care, access to coverage, and improved health.

To improve Medicaid program oversight, CMS is requiring States to submit new files and data elements in T-MSIS which were not collected in MSIS, for the purpose of improving the quality of the data extracts the States submit to CMS on a quarterly or other periodic basis. Following consultation with a wide array of stakeholders, CMS established over 1,000 data elements for T-MSIS. This expands on the approximately 400 data elements collected in MSIS. T-MSIS builds on the original five MSIS files (eligibility and four types of claims: inpatient, long-term care, pharmacy, and other) by adding files for third-party liability, information from managed-care plans, and providers. New T-MSIS Analytic Files (TAF) include: Beneficiary Files: monthly beneficiary summary, annual beneficiary summary, Claims Files: inpatients, long-term care, pharmacy and other files: Provider and Managed Care Files.

Currently, each state submits five extracts to CMS on a quarterly basis. These data are used by CMS to assist in federal reporting for the Medicaid and CHIP. Several reasons culminated in the CMS mission to improve the Medicaid dataset repository, including incomplete data, questionable results, multiple data collections from states, multiple federal data platforms and analytic difficulties in interpreting and presenting the results. In addition, timeliness issues have prompted CMS to re-evaluate its processes and move toward a streamlined delivery, along with an enhanced data repository. The new T-MSIS extract format is expected to further CMS goals for improved timeliness, reliability and robustness through monthly updates and an increase in the amount of data requested.

II. Modifications to SORN 09-70-0541

The following modifications have been made to SORN 09-70-0541 in order to reflect changes to the system of records resulting from the IT system change from MSIS to T-MSIS and to update the SORN generally:

- The SORN has been reformatted to conform to the revised template prescribed in Office of Management and Budget (OMB) Circular A-108, issued December 23, 2016.
- The name of the system of records has been changed from “Medicaid Statistical Information System (MSIS)” to “Transformed - Medicaid Statistical Information System (T-MSIS), HHS/CMS/CMCS.”
- Address information in the System Location and System Manager(s) sections has been updated.
- The Authority section now cites applicable U.S. Code provisions instead of public laws.
- The Purpose section added information collecting over 1000 new data elements to perform expanded data analytics. The T-MSIS data set contains: enhanced information about beneficiary eligibility, beneficiary and provider enrollment, service utilization, claims and managed care data, and expenditure data for Medicaid and CHIP.
- The categories of individuals have not changed, but they are now more clearly delineated as Medicaid recipients and Medicaid providers.
- The Categories of Records section now specifies categories of records, in addition to a listing data elements. Including these categories for the existing five categories, the list has been expanded to add new categories (i.e., files for third-party liability, information from managed-care plans, and providers.) and additional examples of data elements (such as tax identification number/employer identification number (TIN/EIN), national provider identifier (NPI), Social Security Number (SSN), prescriber identification number, and other assigned clinician numbers).

- The Record Source Categories section has added non-Medicare individuals, third party data submitter who are individuals; i.e., Third Party Administrators (TPA); contact persons and authorized representatives (such as parents and guardians of Medicare recipients who are minors) as sources of information.
- The following changes have been made to the Routine Uses section:
 - Two new routine uses have been added, numbered as three and 10.
 - The two breach response-related routine uses which were added February 14, 2018, are now numbered as eight and nine, and
 - CMS grantees were removed from routine use number one.
- There are no changes to the Storage section.
- The Retrieval section now indicates that information will be retrieved by name, address, and Tax Identification Number (TIN) / Employer Identification Number (EIN) pertaining to third party data submitters. Records about contact persons will be retrieved by name, e-mail address and business address.
- The Retention and Disposal section changes retention of Medicaid record to a period of 10 years after the final determination of the case is completed. In addition, any claims-related records encompassed by a document preservation order may be retained longer (i.e., until notification is received from the Department of Justice).
- The Safeguards section has been updated to reflect most recent publications and guidance governing the use and protections of the data maintained in this SOR.
- Records Access, Contesting, and Notification procedures sections has been expanded to provide clarity and better understanding of procedures to follow.

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.*

SYSTEM NAME AND NUMBER: Transformed - Medicaid Statistical Information System
(T-MSIS), HHS/CMS/CMCS, System No. 09-07-0541

SECURITY CLASSIFICATION: Unclassified

SYSTEM LOCATION: The address of the agency component responsible for the system of records is: The CMS Data Center, 7500 Security Boulevard, North Building, First Floor, Baltimore, Maryland 21244–1850 and at various contractor sites.

SYSTEM MANAGER(S): Director, Data and Systems Group, Center for Medicaid and CHIP Services, CMS Mail Stop S2-22-16, 7500 Security Boulevard, Baltimore, Maryland 21244–

1850.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: The specific authority that authorizes the maintenance of the records in the system is given under §1902(a)(6) of the Social Security Act (the Act) (42 United States Code (U.S.C.) 1396a (a)(6)), § 4753(a) (1396a (i)(1)(B)) of the Balanced Budget Act of 1997 (Public Law (Pub.L.) 105– 33), § 4201 of the American Reinvestment and Recovery Act of 2009 (ARRA) (Pub.L. 111–5), and in accordance with §§ 402(c), 1561, 2602, 4302, 6402(c), 6504(a), 6504(b) of the Patient Protection and Affordable Care Act (ACA) (Pub. L. 111–148).

PURPOSE(S) OF THE SYSTEM: The primary purpose of the system is to establish an accurate, current, and comprehensive database containing standardized enrollment, eligibility, and paid claims of Medicaid recipients to be used for the administration of Medicaid at the Federal level, produce statistical reports, support Medicaid related research, and assist in the detection of fraud and abuse in the Medicare and Medicaid programs. T-MSIS will also provide benefits to the states by reducing the number of reports CMS requires of the states, provides data needed to improve beneficiary quality of care, assess beneficiary to care and enrollment, improve program integrity, and support our states, the private market, and stakeholders with key information.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: The records in this system of records are about the following categories of individuals:

- Medicaid recipients (including individuals in the dual eligible population, individuals enrolled in the CHIP program, and non-Medicare individuals);

- Medicaid providers (i.e., physicians and providers of healthcare services to the Medicaid and CHIP population);
- Any non-Medicare individuals whose information is contained in a record about a Medicaid recipient or Medicaid provider;
- Third party data submitters; i.e., third party administrators or independent insurance company personnel who are required to report claims information pertaining to Medicaid recipients, and
- Contact persons such as parents and guardians of Medicare recipients who are minors, CHIP recipients, and non-Medicare individuals.

CATEGORIES OF RECORDS IN THE SYSTEM:

A. The system of records consists of the following categories of records, which contain information about Medicaid recipients and Medicaid providers, and non-Medicaid individuals and contact persons for CHIP recipients and non-Medicare population.

- Original MSIS files:
 - eligibility files
 - Claims files (for inpatient claims, long-term care claims, pharmacy claims, and other claims).
- New Files added to T-MSIS database:
 - third-party liability
 - information from managed care plans
 - providers
- New T-MSIS analytic files (TAF):
 - beneficiary files (monthly beneficiary summary, annual beneficiary summary);

- claims files (for inpatients claims, long-term care claims, pharmacy claims, and other claims);
 - providers of healthcare services to the Medicaid and CHIP population); and
 - Managed Care Plans
- B. Information about Medicaid recipients, includes data elements such as name, address, assigned Medicaid identification number, SSN, Medicare beneficiary identifier (MBI), date of birth, gender, ethnicity and race, medical services, equipment, and supplies for which Medicaid reimbursement is requested. Information will also include the recipient's individually identifiable health information, i.e., health care utilization and claims data, health insurance claim number (HICN), Medicare beneficiary identifier (MBI), and SSN.

Information about Medicaid providers in the above records includes data elements such as contact information (such as the provider's name, address, phone number, e-mail address, date of birth, business address, Tin/EIN, national provider identifier (NPI), SSN, prescriber identification number, and other assigned clinician numbers) and information about health care services the clinician provided to Medicare recipients and the measures and activities the clinician used in providing the services.

Information about any non-Medicaid individuals would include data elements such as those listed above for Medicaid recipients such as name, address, phone number, e-mail address, and SSN or other identifying number.

Information about contact persons for CHIP recipients and non-Medicare individuals includes data elements such as name, address, phone number, e-mail address, TIN/EIN, or other identifying number.

RECORD SOURCE CATEGORIES: Information in the system of records is obtained from State Medicaid agencies or Territories, which collect the information directly from Medicaid recipients or their authorized representatives (such as parents and guardians of Medicare recipients who are minors or from Medicaid providers).

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

- A. The agency may disclose a record about an individual Medicaid recipient or Medicaid provider from this system of records to parties outside HHS, without the individual's prior written consent, pursuant to these routine uses:
1. To support agency contractors, and consultants who have been engaged by the agency to assist in the performance of a service related to the collection and who need to have access to the records in order to perform the activity.
 2. To assist another Federal or state agency, agency of a state government, an agency established by state law, or its fiscal agent to:
 - a. Contribute to the accuracy of CMS' proper management of Medicare/ Medicaid benefits;

- b. Enable such agency to administer a Federal health benefits program, or as necessary to enable such agency to fulfill a requirement of a Federal statute or regulation that implements a health benefits program funded in whole or in part with Federal funds; and/or
 - c. Assist Federal/state Medicaid programs.
- 3. To assist another Federal or state agency, agency of a state government, an agency established by state law, or its fiscal agent to enable such agency to administer a Federal benefits program, or as necessary to enable such agency to fulfill a requirement of a Federal statute or regulation funded in whole or in part with Federal funds.
- 4. To an individual or organization for a research project or in support of an evaluation project related to the prevention of disease or disability, the restoration or maintenance of health, or payment related projects.
- 5. To the Department of Justice (DOJ), court or adjudicatory body when:
 - a. The agency or any component thereof;
 - b. Any employee of the agency in his or her official capacity;
 - c. Any employee of the agency in his or her individual capacity where the DOJ has agreed to represent the employee; or
 - d. The United States Government is a party to litigation or has an interest in such litigation, and by careful review, CMS determines that the records are both relevant and necessary to the litigation and that the use of such records by the

DOJ, court or adjudicatory body is compatible with the purpose for which the agency collected the records.

6. To a CMS contractor (including, but not necessarily limited to fiscal intermediaries and carriers) that assists in the administration of a CMS-administered health benefits program, or to a grantee of a CMS-administered grant program, when disclosure is deemed reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud, waste, and abuse in such program.
7. To another Federal agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States (including any State or local governmental agency), that administers, or that has the authority to investigate potential fraud, waste, and abuse in, a health benefits program funded in whole or in part by Federal funds, when disclosure is deemed reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud, waste, and abuse in such programs.
8. Records may be disclosed to appropriate agencies, entities, and persons when (a) HHS suspects or has confirmed that there has been a breach of the system of records; (b) HHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, HHS (including its information systems, programs, and operations), the Federal government, or national security; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection

with HHS' efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

9. Records may be disclosed to another Federal agency or Federal entity, when HHS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (a) responding to a suspected or confirmed breach or (b) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal government, or national security, resulting from a suspected or confirmed breach.

10. Records may be disclosed to the U.S. Department of Homeland Security (DHS) if captured in an intrusion detection system used by HHS and DHS pursuant to a DHS cybersecurity program that monitors Internet traffic to and from Federal government computer networks to prevent a variety of types of cybersecurity incidents.

B. Additional Circumstances Affecting Routine Use Disclosures: To the extent this system contains Protected Health Information (PHI) as defined by HHS regulation "Standards for Privacy of Individually Identifiable Health Information" (45 Code of Federal Regulations (CFR) Parts 160 and 164, Subparts A and E), disclosures of such PHI that are otherwise authorized by these routine uses may only be made if, and as, permitted or required by the "Standards for Privacy of Individually Identifiable Health Information" (see 45 CFR 164.512(a)(1)).

The disclosures authorized by publication of the above routine uses pursuant to 5 U.S.C. 552a(b)(3) are in addition to other disclosures authorized directly in the Privacy Act at 5 U.S.C. 552a(b)(2) and (b)(4)-(11).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: All records are stored on computer diskette, and magnetic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: The data collected on Medicaid recipients, Medicare beneficiaries (and any non-Medicare individuals) are retrieved by the individual's name, Medicare beneficiary identifier (MBI), health insurance claim number (HICN), SSN, address, and date of birth. The data collected on physicians or providers of services will be retrieved by the provider's name, address, NPI, TIN/EIN and other identifying provider numbers. Information about third party data submitters who are individuals will be retrieved by name, address, and TIN/EIN. Records about contact persons will be retrieved by name, e-mail address and business address.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: CMS will retain identifiable T-MSIS data for a total period not to exceed 10 years after the final determination of the case is completed. The final determination decision encompass the potential timeframe it takes for a claims to be finalized as States can sometimes send incomplete claims data or claims not yet fully covered due to dispute or other considerations for Medicaid eligibility. Any claims-related records encompassed by a document preservation order may be retained longer (i.e., until notification is received from the Department of Justice).

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: CMS has safeguards in place to prevent records from being accessed by unauthorized persons and monitors authorized users to ensure against excessive or unauthorized use. Examples of these safeguards include but not limited to: protecting the facilities where records are stored or accessed with security guards, badges and cameras, securing hard-copy records in locked file cabinets, file rooms or offices during off-duty hours, limiting access to electronic databases to authorized users based on roles and two-factor authentication (user ID and password), using a secured operating system protected by encryption, firewalls, and intrusion detection systems, requiring encryption for records stored on removable media, and training personnel in Privacy Act and information security requirements. Records that are eligible for destruction are disposed of using destruction methods prescribed by NIST SP 800-88. Personnel having access to the system have been trained in the Privacy Act and information security requirements. Employees who maintain records in the system are instructed not to release data until the intended recipient agrees to implement appropriate management, operational and technical safeguards sufficient to protect the confidentiality, integrity and availability of the information and information systems, and to prevent unauthorized access.

The Information Technology (IT) system used to house the records conforms to all applicable Federal laws and regulations and Federal, HHS, and CMS policies and standards as they relate to information security and data privacy. These laws and regulations may apply but are not limited to: the Privacy Act of 1974; the Federal Information Security Management Act of 2002; the Federal Information Security Modernization Act of 2014; the Computer Fraud and Abuse Act of 1986; the Health Insurance Portability and Accountability Act of 1996; the E-Government Act of

2002; the Clinger-Cohen Act of 1996; the Medicare Modernization Act of 2003; and the corresponding implementing regulations.

OMB Circular A-130, Management of Federal Resources, and Security of Federal Automated Information Resources also applies to the SOR. Federal, HHS, and CMS policies and standards include but are not limited to: All pertinent National Institute of Standards and Technology publications; the HHS Information Security and Privacy Policy Handbook (IS2P), the CMS Acceptable Risk Safeguards (ARS), and the CMS Information Security and Privacy Policy (IS2P2).

RECORD ACCESS PROCEDURES: An individual seeking access to a record about him/her in this system of records must submit a written request to the System Manager indicated above. The request must contain the individual's name and particulars necessary to distinguish between records on subject individuals with the same name, such as NPI or TIN, and should also reasonably specify the record(s) to which access is sought. To verify the requester's identity, the signature must be notarized or the request must include the requester's written certification that he/she is the person he/she claims to be and that he/she understands that the knowing and willful request for or acquisition of records pertaining to an individual under false pretenses is a criminal offense subject to a \$5,000 fine.

CONTESTING RECORD PROCEDURES: Any subject individual may request that his/her record be corrected or amended if he/she believes that the record is not accurate, timely, complete, or relevant or necessary to accomplish a Department function. A subject individual making a request to amend or correct his record shall address his request to the System Manager

indicated, in writing, and must verify his/her identity in the same manner required for an access request. The subject individual shall specify in each request: (1) The system of records from which the record is retrieved; (2) The particular record and specific portion which he/she is seeking to correct or amend; (3) The corrective action sought (e.g., whether he/she is seeking an addition to or a deletion or substitution of the record); and, (4) His/her reasons for requesting correction or amendment of the record. The request should include any supporting documentation to show how the record is inaccurate, incomplete, untimely, or irrelevant.

NOTIFICATION PROCEDURES: Individuals wishing to know if this system contains records about them should write to the System Manager indicated above and follow the same instructions under Record Access Procedures.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY:

- Medicaid Statistical Information System (MSIS), System No. 09-07-0541 last published in full at 71 FR 65527 (Nov. 8, 2006), as amended 78 FR 32257 (May 29, 2013), and updated 83 FR 6591 (Feb. 14, 2018).