Billing Code: 4120-03

DEPARTMENT OF HEALTH AND HUMAN 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 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 national Medicaid dataset, consisting of standardized enrollment, eligibility, and paid claims data about Medicaid recipients which 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 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 United States Code (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 Blvd., 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 Blvd., Baltimore, MD 21244; telephone number (410) 786-9828; e-mail address 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 that houses the national Medicaid dataset. It is a joint effort by the states and CMS to build an improved 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 and CHIP programs 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, consisting of eligibility files and four types of claims files (inpatient, long-term care, pharmacy, and other), by adding files for third-party liability, managed-care plans, and Medicaid providers, and by adding T-MSIS analytic files (TAF).

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 Children's Health Insurance Program (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 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 42 U.S.C. 1396b(r) in place of a public law citation and includes one new authority, 42 U.S.C. 18001, et seq.
- The Purpose section has been revised to omit a summary of the routine uses and to include additional purposes for which T-MSIS records may be used ("reduce the number of reports CMS requires of the states, provide data needed to improve beneficiary quality of care, improve program integrity, and support the states, the private market, and stakeholders with key information").
- The Categories of Individuals section, which was previously limited to Medicaid recipients and Medicaid providers, now also includes non-Medicaid individuals, third party data submitters, and contact persons.
- The Categories of Records section now specifies categories of records in addition to listing data elements; groups the data elements by category of individual; adds name, address, phone number, TIN/EIN, NPI, MBI and "information about health care services the clinician provided to Medicaid recipients and the measures and activities the clinician used in providing the services;" and omits "information used to determine whether a sanction or suspension is warranted."
- The Record Source Categories section now describes the sources as "state Medicaid agencies

or territories, which collect the information directly from Medicaid recipients or their providers or other authorized representatives" (instead of as state Medicaid agencies and systems and CMS Form 2082).

- The following changes have been made to the Routine Uses section:
  - In routine use 2, at c., redundant wording ("within the state") has been removed after the phrase "assist federal/state Medicaid programs."
  - Routine use 5 has been revised to omit unnecessary wording limiting the disclosures to uses "compatible with the purpose for which the agency collected the records." (The wording is unnecessary because it restates the definition of a routine use.)
  - One new routine use has been added, numbered as 3, which permits disclosures to support federally-funded benefit programs.
  - The fraud, waste, and abuse routine use which was added May 29, 2013 is now numbered as 8.
  - The two breach response-related routine uses which were added February 14, 2018 are now numbered as 9 and 10.
- The Storage section now states that records are stored "in an information technology (IT) system" (instead of "on computer diskette and magnetic media").
- The Retrieval section previously listed these personal identifiers: beneficiary identification number, social security number (SSN), HICN, and provider identification number. It now groups the identifiers by category of individual and includes additional identifiers (e.g., MBI and NPI).
- The Retention and Disposal section has been revised to state that identifiable "T-MSIS" data will be retained "for a period of 10 years" after the final determination of "the applicable

enrollment, eligibility, or claim" is completed (instead of stating that identifiable "MSIS" data will be retained "for a total period not to exceed 10 years" after the final determination of "the case" is completed).

- The Safeguards section has been updated to list examples of applicable safeguards (security guards, badges and cameras, locks, limiting user access based on roles and two-factor authentication, encryption, firewalls, intrusion detection systems).
- The procedures for making access, correction and amendment, and notification requests have been revised. In the previous iteration of the SORN, the verification procedures required the individual's name (woman's maiden name, if applicable). The individual had the option of furnishing the SSN to prevent delay in locating the record(s). The new process to verify identity requires a notarized signature or a statement under penalty of perjury (instead of requiring name and` woman's maiden name if applicable). Additionally, in order to locate the record(s), the individual's name and SSN are now required (previously, SSN was optional for this purpose).

Signed:

Barbara Demopulos,
Privacy Advisor,
Division of Security, Privacy Policy and Governance,
Information Security and Privacy Group,
Office of Information Technology,
Centers for Medicare & Medicaid Service.

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 Blvd. North Bldg., First Floor, Baltimore, MD 21244–1850.

SYSTEM MANAGER(S):

Director, Data and Systems Group, Center for Medicaid and CHIP Services, CMS Mail Stop S2-22-16, 7500 Security Boulevard, Baltimore, MD 21244–1850, telephone number (410) 786-9361.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

42 U.S.C. 1396a(a)(6), 1396b(r), and 18001 et seq.

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 data about 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 reduce the number of reports CMS requires of the states, provide data needed to improve beneficiary quality of care, improve program integrity, and support the 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-Medicaid individuals);
- Medicaid providers (i.e., physicians and providers of healthcare services to the Medicaid and CHIP population);
- Any non-Medicaid 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 Medicaid recipients who are minors, CHIP recipients, and non-Medicaid individuals.

CATEGORIES OF RECORDS IN THE SYSTEM:

The categories of records are:

- Original MSIS files:

    - eligibility files
    - claims files (for inpatient, long-term care, pharmacy, and other claims)
- New files added to T-MSIS database:
    - third-party liability
    - managed care plans
    - Medicaid providers
- New T-MSIS analytic files (TAF):
    - beneficiary files (monthly beneficiary summary, annual beneficiary summary)
    - claims files (for inpatient, long-term care, pharmacy, and other claims)
    - providers of healthcare services to the Medicaid and CHIP population; and
    - managed care plans

Data elements about each category of individual may include the following:

- *Medicaid recipients*: name, address, assigned Medicaid identification number, social security number (SSN), Medicare beneficiary identifier (MBI), date of birth, gender, ethnicity and race, medical services, equipment, and supplies for which Medicaid reimbursement is requested, individually identifiable health information (i.e., health care utilization and claims data), and health insurance claim number (HICN).
- *Medicaid providers*: name, address, phone number, e-mail address, business address, date of birth, tax identification number/employer identification number (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

Medicaid recipients and the measures and activities the clinician used in providing the services.

- *Any non-Medicaid individuals*: name, address, phone number, email address, and SSN or other identifying number.
- *Third party data submitters*: name, address, phone number, and email address.
- *Contact persons*: name, address, phone number, email 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 providers or other authorized representatives (such as parents and guardians of Medicaid recipients who are minors).

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

The agency may disclose a record about an individual record subject 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, consultants, or CMS grantees 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.

6. To a CMS contractor (including fiscal intermediaries and carriers) assisting 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. To disclose to health plans, defined for this purpose as plans or programs that provide health benefits, whether directly, through insurance, or otherwise, and including—(1) a policy of health insurance; (2) a contract of a service benefit organization; and (3) a membership agreement with a health maintenance organization or other prepaid health plan, 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, or abuse in such programs. Disclosures may include provider and beneficiary-identifiable data.
9. 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.

10. 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.

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 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 in an information technology (IT) system.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

All data collected on Medicaid recipients, Medicare beneficiaries, and any non-Medicaid 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 Medicaid providers will be retrieved by the provider's name, address, National Provider Identifier (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 period of 10 years after the final determination of the applicable enrollment, eligibility, or claim is completed. 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: 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. Before disclosing records to a party outside CMS, CMS requires the intended recipient 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.

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 from an agency under false pretenses is a criminal offense subject to a $5,000 fine. Additionally, in order to locate the record(s), the individual's name and SSN are required.

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, must verify his/her identity in the same manner required for an access request, and must provide his/her name and SSN for the purpose of locating the record. 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:

71 FR 65527 (Nov. 8, 2006), 78 FR 32257 (May 29, 2013), 83 FR 6591 (Feb. 14, 2018).

[FR Doc. 2019-01157 Filed: 2/5/2019 8:45 am; Publication Date: 2/6/2019]