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 new system of records.

SUMMARY: In accordance with the Privacy Act of 1974, as amended, the Department of Health and Human Services (HHS) is establishing a new system of records to be maintained by the Centers for Medicare & Medicaid Services (CMS), titled "Nurses for Nursing Homes Program (NNHP)," system No. 09-70-0545. The new system of records will cover the collection of records on individuals who apply for, participate in, or otherwise support the Nurses for Nursing Homes Program (NNHP). Records maintained in the system will include personally identifiable information (PII), including demographic, professional licensure and credential information, education and training information, employment and nursing facility affiliation, payment information, tax reporting, audit records, and other records necessary to administer the program.

CMS will use these records to support the administration of a nursing workforce incentive program designed to strengthen the workforce serving Medicare and Medicaid-certified nursing homes with a focus on underserved and rural communities. The scope of the new system of records will be commensurate with its purpose of supporting the Nursing Home Staffing Campaign/Nursing Incentive Program (NHSC/NIP).

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this new system of records is effective **[INSERT DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**, subject to a 30-day period in which to comment on this new system of records described below. Submit

any comments by **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**.

ADDRESSES: The public should submit written comments on this notice, by mail or email, to Barbara Demopulos, CMS Privacy Act Officer, 7500 Security Blvd., N1-14-56, Baltimore, MD 21244-1850, or barbara.demopulos@cms.hhs.gov. To review comments, please contact Barbara Demopulos.

FOR FURTHER INFORMATION CONTACT: General questions about the system of records should be addressed to: Evan Shulman, Director, Division of Nursing Homes, CMS Division of Security, Privacy Policy & Oversight (DSPPO), Information Security & Privacy Group (ISPG), Office of Information Technology (OIT), 7500 Security Blvd., Baltimore, MD 21244-1850. Office: 443-324-9561 or email evan.shulman@cms.hhs.gov.

SUPPLEMENTARY INFORMATION:

I. Background on the CMS Nurses for Nursing Homes program:

The Nurses for Nursing Homes program is a new CMS initiative launched under the authority of the Office of the Administrator. Eligible nurses apply to the Program through the CMS Nurses for Nursing Homes Program application portal, where CMS personnel review and validate applicant eligibility, verify nursing licensure and employment, and place confirmed participants at eligible nursing facilities (i.e., CMS-certified nursing homes that meet the Program's participation criteria, including those serving underserved and rural communities). Participating nursing facility employer representatives periodically provide employment verification and compliance updates, while CMS personnel oversee financial administration, including the processing of quarterly incentive payments and required tax reporting. Financial incentives may include student loan repayment and incentive stipends, paid out quarterly over the CMS-established commitment period. The program is funded through Civil Monetary Penalties (CMPs) collected from Medicare and Medicaid certified nursing homes for health and safety

violations, authorized under Title XVIII, Section 1819(h)(2)(B)(ii)(IV)(ff) and Title XIX, Section 1919(h)(2)(B)(ii)(IV)(ff) of the Social Security Act, and codified at 42 CFR 488.433.

II. New System of Records 09-70-0545:

This is a new system of records. No existing CMS SORN covers this program, its data collection, routine uses, or this population of records (individual nurse applicants, not Medicare/Medicaid providers or beneficiaries). A report on this new system of records has been sent to OMB and Congress in accordance with 5 U.S.C. 552a(r).

Barbara Demopulos,
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 (CMS).

SYSTEM NAME AND NUMBER:

Centers for Medicare & Medicaid Services (CMS) Nurses for Nursing Homes Program, System No. 09-70-0545.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

The address of the agency component responsible for this system of records is: Centers for Medicare & Medicaid Services, U.S. Department of Health and Human Services, 7500 Security Blvd., Baltimore, MD 21244-1850.

SYSTEM MANAGER(S):

The system manager is the Chief Technology Officer, Office of Health Technology & Products (OHTP) at Centers for Medicare & Medicaid Services, U.S. Department of Health and Human Services, 7500 Security Blvd., Baltimore, MD 21244-1850.

Program Point of Contact: Director, Division of Nursing Homes Centers for Medicare & Medicaid Services, U.S. Department of Health and Human Services, 7500 Security Blvd., Baltimore, MD 21244-1850.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The statutory authority to maintain this system of records is given under:

- Title XVIII, Section 1819(h)(2)(B)(ii)(IV)(ff) of the Social Security Act, Medicare nursing facility standards and Civil Monetary Penalty authority;
- Title XIX, Section 1919(h)(2)(B)(ii)(IV)(ff) of the Social Security Act, Medicaid nursing facility standards and Civil Monetary Penalty authority;
- 42 CFR 488.433, Civil Monetary Penalties (CMPs) collected from Medicare and Medicaid certified nursing homes for health and safety violations;
- 31 U.S.C. 7701(c), Debt Collection Improvement Act of 1996, Requirement That Applicant Furnish Taxpayer Identifying Number; and
- OMB Circular A-123, Internal controls and financial management.

PURPOSE(S) OF THE SYSTEM:

Relevant agency personnel use records about individuals in this system of records on a need-to-know basis for the following purposes:

1. To identify and select qualified RNs and LPNs/LVNs to participate in the Program, including verifying initial eligibility based on nursing licensure, employment at a qualifying CMS-certified nursing facility, and commitment to a CMS-established service period;
2. To maintain and verify program applicant and participant credentials, nursing licensure, and employment data to confirm that all claimed background and employment

information is valid and all credentials are current and in good standing throughout the duration of the service commitment;

3. To administer financial incentive payments, including student loan repayment awards and incentive stipends, disbursed quarterly over the CMS-established commitment period via an Automated Clearing House/ Electronic Funds Transfer (ACH/EFT) payment rails;
4. To process and issue federal tax reporting documentation, including Form 1099, for incentive payments made to participating nurses, and to fulfill related obligations to the Internal Revenue Service (IRS) and Department of the Treasury;
5. To respond to inquiries from program applicants, participants, their authorized representatives, and Congressional representatives regarding application status, payment processing, eligibility determinations, and service commitment compliance;
6. To compile and generate managerial, compliance, and statistical reports related to program administration, payment tracking, and participant compliance with service requirements;
7. To monitor participating nurses' ongoing compliance with service commitment requirements at eligible CMS-certified nursing facilities, including periodic verification of hours worked, employment status, and continued facility eligibility
8. To detect and prevent duplicate or fraudulent applications through Social Security number (SSN)-based duplicate detection, nursing license verification, and identity proofing via Identity Assurance Level 2 (IAL2)-certified Credential Service Providers, consistent with Routine Use 1 (contracted services assisting CMS in carrying out program functions) and Routine Use 3 (disclosures to agencies responsible for enforcing, investigating, or prosecuting violations);
9. To facilitate state Medicaid agency fund transfers related to the Program's financial administration, to support enrollment reporting to state agencies for participating nurses

and facilities, and to provide payment reporting to state agencies as required by applicable program and Medicaid requirements; and

10. To maintain audit logs, including IP address and device data, for fraud detection and system security purposes from all users accessing the Program portal and CMS-operated systems in accordance with Federal Information Security Modernization Act and National Institute of Standards and Technology requirements.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

1. RNs and LPNs/LVNs who have applied for, are receiving, or have received financial incentive payments, including student loan repayment awards and incentive stipends, under the Nurses for Nursing Homes program .
2. Representatives of participating CMS-certified nursing facilities who interact with the Facility Portal for employment verification and vacancy management purposes.

CATEGORIES OF RECORDS IN THE SYSTEM:

The categories of records maintained in this system include program applications and associated forms, documents, reports, correspondence, and payment records for the Nurses for Nursing Homes program. Data elements contained within these records include:

- Identity information: full legal name, date of birth, home address, personal email address, personal phone number, SSN/Taxpayer Identification Number (TIN), and identity proofing verification data collected through Identity Assurance Level 2 (IAL2)-certified Credential Service Providers; and
- Education and training information: nursing degree(s), institution(s) attended, graduation date(s), and relevant training certifications;
- Employment information: nursing license number and issuing state, employer name, nursing facility information including entity legal name, service/practice locations, CMS Certification Number (CCN), and nursing facility employer representative contact information (name, title, email address, and phone number) for individuals authorized to

access the Facility Portal and submit employment verification and compliance updates on behalf of the facility; employment records; hours worked.

- Financial information:
    - Bank account and routing numbers for Automated Clearing House/Electronic Funds Transfer (ACH/EFT) disbursement;
    - Incentive payment amounts and disbursement records; and
    - Tax record information (Form 1099 tax records);
- Student loan information: loan account number(s), loan balance, account status, and other information necessary to identify the and his/her loans for repayment purpose; and
- System and audit data: IP address and device data collected for fraud detection and audit logging purposes.

RECORD SOURCE CATEGORIES:

Records in this system are obtained directly from the subject individuals (i.e., nurse applicants and participants who provide their own personal, professional, and financial information in connection with their application and participation in the Program), as well as from the following third-party sources:

- Participating nursing facilities and their authorized employer representatives, for employment verification, hours worked, and compliance reporting;
- CMS-approved Credential Service Providers, for identity attributes used in authentication and identity proofing;
- National Government Services (NGS/Wellpoint), for payment processing data;
- The Internal Revenue Service (IRS) and the Department of the Treasury, for TIN/SSN verification and tax reporting; and

State agencies, for enrollment and payment reporting related to state fund transfers.

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

The Privacy Act at 5 U.S.C. 552a(b)(3) allows us to disclose information to parties outside the agency without the subject individual's consent for a purpose that is compatible with the purpose(s) for which the information was collected, if a description of the disclosure is published as a "routine use" in the applicable System of Records Notice (SORN). The disclosures authorized by routine uses published 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), which can also be made without the subject individual's consent.

The following routine uses are published for this system of records:

1. To support agency contractors, consultants, or others who have been engaged by the agency to assist with the accomplishment of a CMS function relating to the purposes of this system of records and who need to have access to the records to assist CMS, including the CMS-contracted companies or 3rd party services used for ACH/EFT payment disbursements, financial operations, payment processing and tax reporting.
2. To the Department of Justice (DOJ) or to a court or other tribunal when HHS, or any component thereof, or any HHS employee in his or her official or individual capacity, or the United States Government, is a party to litigation or other proceedings and has an interest in such proceedings, and by careful review, HHS determines that the records are both relevant and necessary to the proceedings.
3. To another federal agency or 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 a violation or potential violation of law, whether civil, criminal, or regulatory in nature, otherwise, responsible for enforcing, investigating, or prosecuting such violation, if the information is relevant to the enforcement, regulatory, investigative, or prosecutorial responsibility of the receiving entity.

4. To the Internal Revenue Service (IRS) and the Department of the Treasury for federal tax reporting purposes, including W-2 (or Form 1099, pending final legal determination) issuance and Taxpayer Identification Number (TIN) verification, in accordance with applicable IRS regulations.
5. To CMS-contracted 3rd party services for the purpose of verifying the employment status and hours worked by nurse applicants and participants at participating nursing facilities.
6. To the CMS-contracted 3rd party services for the purpose of verifying the nursing licensure, credentials, and eligibility of nurse applicants and participants.
7. To state agencies for enrollment and payment reporting purposes and to facilitate state fund transfers related to the Nurses for Nursing Homes program.
8. To lending institutions and loan servicing agencies for the purpose of obtaining payoff balances on applicant and participant educational loans and determining whether loans are eligible for repayment under the program.
9. To the IRS about an individual applying under the program to determine if the applicant has a delinquent tax debt. This disclosure is for the sole purpose of determining the applicant's eligibility for funding.
10. To the HHS Office of Inspector General (OIG) or the Government Accountability Office (GAO) for audit, oversight, and program integrity purposes.
11. To appropriate agencies, entities, and persons when (1) HHS suspects or has confirmed that there has been a breach of the system of records, (2) 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 (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with HHS's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

12. 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 (1) responding to a suspected or confirmed breach or (2) 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.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are stored in hard copy files and/or electronic systems or media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are retrieved by one or more of the following personal identifiers: participant full legal name; SSN or TIN; date of birth; nursing license number and issuing state; employer/facility CCN; Credential Service Provider identifiers or email address; and payment record number or Applicant/Participant ID number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

The applicable schedules approved by the National Archives and Records Administration (NARA) is DAA-0440-2015-0008-0001 (Bucket 6) – Provider and Health Plan records, which includes provider applications and certifications; health plan records; program review and audit records; hearing files; and administrative records to be destroyed no sooner than seven years after cut-off, but longer retention is authorized.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Safeguards conform to the HHS Information Security and Privacy Program, https://www.hhs.gov/ocio/securityprivacy/index.html. Information is safeguarded in accordance with applicable laws, rules and policies, including the HHS Information Technology Security Program Handbook; the E-Government Act of 2002, which includes the Federal Information

Security Management Act of 2002 (FISMA), 44 U.S.C. 3541-3549, as amended by the Federal Information Security Modernization Act of 2014, 44 U.S.C. 3551-3558; all pertinent NIST publications, and OMB Circular A-130, Managing Information As a Strategic Resource.

Records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. 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 access control mechanisms (i.e., username and password credentials), 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, as revised.

RECORD ACCESS PROCEDURES:

An individual seeking access to records about the individual in this system of records must submit a written access request to the applicable System Manager identified in the "System Manager" Section indicated above. An access request must contain the requester's full name, address, email address or other contact information, and signature. To verify the requester's identity, the signature must be notarized, or the request must include the requester's written certification that the requester is the person the requester claims to be and that he/she understands that the knowing and willful request for or acquisition of a record pertaining to an individual under false pretenses is a criminal offense subject to a fine of up to $5,000. An individual may also request an accounting of disclosures that have been made of the records about the individual, if any.

CONTESTING RECORD PROCEDURES:

An individual seeking to amend a record about the individual in this system of records must submit a written amendment request to the System Manager identified in the "System Manager(s)" section. The request must contain the same information required for an access request, and must reasonably identify the record, specify the information contested, state the corrective action sought, provide the reasons for the amendment, and include any supporting justification or documentation. The individual must verify his or her identity in the same manner required for an access request. The right to contest records is limited to information that is factually inaccurate, incomplete, irrelevant, or obsolete.

NOTIFICATION PROCEDURES:

An individual who wishes to know if this system of records contains records about the individual must submit a written request to the System Manager identified in the "System Manager(s)" section. The request must contain the same information required for an access request, and the individual must verify their identity in the same manner required for an access request; see "Records Access Procedures" above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

[FR Doc. 2026-17005 Filed: 8/19/2026 8:45 am; Publication Date: 8/20/2026]