<u>Supporting Statement – Part A</u>

CMS Identity Management (IDM) System
(CMS-10452; OMB-0938-1236)

A. Background

In support of the American Recovery and Reinvestment Act (ARRA), the Health Information Technology for Economic and Clinical Health Act (HITECH), the Patient Protection and Affordable Care Act (PPACA) of 2010, also known as Affordable Care Act (ACA), and the Medicare Access & CHIP Reauthorization Act (MACRA) of 2015, Centers for Medicare & Medicaid Services (CMS) has implemented an Enterprise Identity Management (EIDM) system. EIDM is an identity management system that provides the means for users needing access to CMS applications to identify themselves, apply for and receive credentials in the form of a user identifier (User ID) and password, and apply for and receive approval to access the required application/system(s). EIDM manages the life cycle of user ID's, passwords and the supporting data collected from the user, from issuance to archive.

CMS has moved from this centralized on premise model for enterprise identity management to a cloud-based solution, IDM, with multiple products providing specialized services: Okta Identity as a Service (IDaaS), which includes Multi-Factor Authentication (MFA) services; Experian Remote Identity Proofing (RIDP) services; and Cloud Computing Services-Amazon Web Services/ Information Technology Operations (CCS-AWS/ITOps) Hub Hosting. The path to production for IDM was implemented in three (3) phases, with the last phase successfully deployed into production on 2/19/2021. CMS is currently procuring an IDM Continuous Integration/Continuous Delivery (CI/CD) contractor to provide oversight, guidance, and direction to ensure all IDM products and services are functioning as expected, and to make improvements and enhancements to IDM as the system matures and is maintained in an Agile-centric environment. Additionally, CMS has begun the decommissioning of the legacy EIDM system and expects to have the system sunsetted by the end of March 2021. Similar to EIDM, IDM will provide the same identity management capabilities (i.e., authentication, authorization, and life cycle management) and will support over two-hundred (200) CMS business applications.

IDM provides the following services:

1. Registration Service – This function allows new users to create an account credential in order to obtain a single digital identity that can be used across CMS applications that are integrated with IDM. As part of the registration and authentication processes, IDM invokes Remote Identity Proofing (RIDP) using a third-party solution provided by Experian Precise ID to ensure authenticity of the claimed identity. The service provided by Experian has been customized to support CMS.

2. Authentication Service – This function confirms the user's identity attributes and access privileges. It is available only to users that have completed the registration process and have a valid credential. As part of the authentication process, IDM invokes Multi-Factor Authentication (MFA), by which IDM requires (when appropriate) that the user of a CMS business application provide more than one form of credential in order to verify their identity as a condition for system access. Identity Authentication and Multi-Factor Authentication (MFA) services are provided by Okta's cloud Identity as a Service (IDaaS).
3. Role Management and Workflow Authorization Service – This function, performed by Activiti (an open-source business automation tool), is used to manage IDM's role service workflow and process management tool to support the authorization part of the IDM solution along with Okta.
4. Lifecycle Management Service – This function includes self-service management, which allows user information to change over time in a controlled and auditable manner within IDM. User information can be managed by the user through self-service or by an Authorized Help Desk user (e.g., reset password, update user profile, etc.).

The information collected will be gathered and used solely by CMS, approved contractor(s), and state health insurance exchanges to prove the identity of an individual requesting electronic access to CMS protected information or services. Information confidentiality will conform to the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the Federal Information Security Management Act (FISMA) requirements. Respondents may also access CMS' Terms of Service and Privacy Statement on the CMS Portal and IDM websites.

This is \a Reinstatement without change type of approval request for the Centers for Medicare and Medicaid Services (CMS) Identity Management (IDM) system. The transition, or more accurately, rebranding of the current identity management system did not result in changes to this package's requirements, collection methods, policies, or burden. As stated above, CMS expects the EIDM system to be fully decommissioned by this PRA package's current expiration date of 3/31/2021. Therefore, CMS requests the removal of the EIDM system from this PRA package.

B. Justification

1. Need and Legal Basis

HIPAA regulations require covered entities to verify the identity of the person requesting Personal Health Information (PHI) and the person's authority to have access to that information. Per the HIPAA Security Rule, covered entities, regardless of their size, are required under Section164.312(a)(2)(i) to "assign a unique name and/or number for identifying and tracking user identity." A 'user' is defined in Section 164.304 as a "person or entity with authorized access". Accordingly, the Security Rule requires covered entities to assign a unique name and/or number to each employee or workforce member who uses a system that receives, maintains or transmits electronic PHI, so that system access and activity can be identified and tracked by user. This pertains to workforce members within health plans, group health plans, small or large provider offices, clearinghouses and beneficiaries.

Federal law requires that CMS take precautions to minimize the security risk to the Federal information system. FIPS PUB 201 – 1 Para 1.2: “Homeland Security Presidential Directive 12 (HSPD 12), signed by the President on August 27, 2004, established the requirements for a common identification standard for the identification of credentials issued by Federal Departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. HSPD 12 directs the department of Commerce to develop a Federal Information Processing Standards (FIPS) publication to define such a common identification credential.”

OMB-04-04 updates guidance issued by OMB under the Government Paperwork Elimination Act of 1998, 44 U.S.C. § 3504 and implements section 203 of the E-Government Act, 44 U.S.C. ch. 36. After determining the assurance level appropriate for access to government systems or information, “the agency should refer to the National Institute of Standards and Technology (NIST) e-authentication technical guidance to identify and implement the appropriate technical requirements. “NIST SP 800-63-2 is the authoritative document that provides information on the technical controls and approaches that an Agency must use for remote as well as in-person identity proofing requirements from Levels of Assurance (LOA) 1 through 4. Currently, Federal Identity, Credential, and Access Management (FICAM) does not have a certification process for a stand-alone identity proofing capability; current FICAM certification, via the Trust Framework Adoption Process, applies to a combined identity proofing-credential issuance solution. As such, the requirements levied on an Identity Proofing service are based on the foundational requirements that all US Government Agencies must follow in complying with NIST Guidance.

OMB-O4-04 requires that data collection must comply with the Privacy Act but also states:

Most e-authentication processes capture the following information:

- *Information regarding the individuals/ businesses/governments using the E-Gov. service;*
- *Electronic user credentials (i.e., some combination of public key certificates, user identifiers, passwords, and Personal Identification Numbers);*
- *Transaction information associated with user authentication, including credential validation method;*
- *Audit Log/Security information.*

According to section 1321(c) of the PPACA, the Secretary has the authority to determine whether a State Exchange meets the requisite standards to operate. If the Exchange fails to meet these standards, the Secretary may establish and operate a Federally-facilitated Exchange (FFE) in that State. The FFE will be required to meet the same requirements as the state exchanges, including:

- Exchanges must be able to accept application information through secure electronic interfaces and determine eligibility promptly regardless of which agency received the application (CMS 9989-F Sec 155.345)
- Exchanges must establish privacy and security standards that protect PII (Personally Identifiable Information) data collected and stored by the Exchanges and States, while allowing applicants access to their data. This includes authenticating users, monitoring and mitigating security issues, developing secure interfaces with partners (CMS-9989-F Sec 155.260).
- Exchanges must submit name, date of birth and SSN (Social Security Number) of each enrollee to Social Security Administration (SSA) to verify eligibility information. If an enrollee attests to being a legal alien or SSA records indicate inconsistencies, Exchanges will submit name, date of birth and any other information submitted to Department of Homeland Security (DHS). Information must also be submitted to the Dept. of Treasury to determine if applicant is eligible for a tax credit or cost-sharing reduction. If eligibility information cannot be verified or if inconsistencies exist, procedures are defined. (ACA 1411(a)(5)(c)(2) and CMS 9989-F Sec 155.315).

ARA/HITECH CFR 45 **§** 164.312 Technical Safeguards states:

A covered entity must, in accordance with § 164.306:

(a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

(2) Implementation specifications: (i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.

Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency. IDM should:

- Support all currently approved Federal Identity, Credential, and Access Management (FICAM) Protocol Profiles, as found on IDManagement.gov, for browser based Simplified Sign-On (SSO) [OpenID 2.0 and SAML 2.0 required; Identity Metasystem Interoperability version 1.0 (IMI 1.0) support is optional]
- Support newly approved FICAM Protocol profiles, as found on IDManagement.gov, within [90 days] of final approval by the Identity, Credential, And Access Management Subcommittee (ICAMSC)

- Be capable of supporting all FICAM Adopted Trust Framework Provider Approved Credential Providers as found on IDManagement.gov
- Be capable of supporting PIV (for Government-to-Government use cases) and Personal Identity Verification Interoperable (PIV-I) Authentication which includes Trust Path Discovery and Trust Path Validation functionality
- Support the FICAM Security Assertion Markup Language version 2.0 (SAML 2.0) Identifier and Protocol Profiles for Backend Attribute Exchange version 2.0 (BAE v2.0) and the associated FICAM SAML 2.0 Metadata Profile for BAE v2.0 if the solution implements a SAML 2.0 Attribute Query/Response mechanism
- Support the following protocols and assertion formats for web service communication between itself and the relying party Agency application:

  o Protocols: Hypertext Transfer Protocol Secure (HTTPS), SAML 2.0 o Assertion Formats: SAML 2.0, Extensible Markup Language (XML), JavaScript Object Notation (JSON), Representational State Transfer (REST), Simple Object Access Protocol (SOAP).

2. Information Users

In order to prove the identity of an individual requesting electronic access to CMS protected information or services, IDM (leveraging Experian Precise ID RIDP services) will collect a core set of attributes about that individual. These core attributes will be used to:

1. Provide the user a CMS issued IDM ID and password;
2. Provide CMS with additional data (i.e., personal, self-identifying questions and answers) collected and authenticated for multi-factor identification;
3. Provide the identity proofing service sufficient data to establish that the individual's identity is provable to a NIST assurance level;
4. Store the approval information returned by the identity proofing service;
5. Authenticate the user;
6. Authorize the user for application access.

Data collection and verification occurs in four (4) phases:

- **Phase 1:** During this phase, the initial form data is collected from the end user requesting a CMS digital account credential. Phase 1 required attributes include full legal name, current or most recent personal address, primary phone number, email address, user ID/name, password, and date of birth. The user will also be required to select one (1) knowledge-based authentication question and provide a corresponding answer to the question, which IDM will collect and use for additional security as part of self-service activities and password resets. The user is required to answer the question correctly in order to reset a password and account unlock functionality.

- **Phase 2:** In this phase, the user logs into the CMS portal/application website by entering their CMS IDM credential and password created in Phase 1. The user then proceeds to the CMS business application catalogue to select an application and then to request a role(s) in order to obtain access to that CMS application. Each business application role has a NIST Level of Assurance (LOA) associated with it. As part of the approval workflow, the user may be required to enter additional attributes (e.g., business organization/contact information, contract number, reason for request, etc.).

- **Phase 3:** Once the user has filled in the required application specific information required in Phase 2, the user's legal name, address, phone, date of birth provided in Phase 1 will be transmitted to the Remote Identity Proofing (RIDP) service provider to uniquely identify the user and ensure they are who they claim to be. Based on the LOA associated with the business application role being requested, the user's full SSN will be collected. A user's SSN is only required for LOA 3; however, the user has the option of providing their SSN in spite of this requirement. Additionally, also predicated on the LOA associated with the business application role being requested, the user will be presented with a list of four (4) to six (6) Out-of-Wallet Questions (OOW), provided by the RIDP service provider, to answer. The questions and the answers provided by the user are managed by the RIDP service provider and are not retained by the CMS IDM system. The RIDP service provider only returns to IDM the results of the online proofing transaction (i.e., reference ID, a unique cross-reference ID, date, proofing score, and a pass/fail code). Once the end users' identity is confirmed by the RIDP service provider, the user can proceed to Phase 4 to setup additional security for their account.

- **Phase 4:** In this phase, depending on the LOA associated with the business application role, the user may be required (or can voluntarily select) to complete the multi-factor authentication (MFA) registration process. MFA provides an extra layer of security to a user's account, such as a one-time use security code, when logging in with a User ID and Password. Email is automatically setup as the default MFA Factor for all users required to login with MFA. No further action is necessary by users to setup email as their MFA Factor. Users may add other MFA Factors by selecting Manage/View MFA from the My Profile menu page.

3. Use of Information Technology

In compliance with the Government Paperwork Elimination Act (GPEA), which requires Federal agencies, by October 21, 2003, "to provide individuals or entities the option to submit information or transact with the agency electronically and to maintain records electronically when practicable" and "specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form," IDM has mandated that all data collection efforts (e.g., end-user account registration, recertification, or profile updates) on the CMS Portal website are conducted electronically 100% of the time. IDM does not require a signature from respondents for this collection.

IDM will save money and reduce operational burden to the Government by deploying an enterprise-wide, distributed cloud- and application programming interface (API)-based identity and access management system. IDM should:

1. Reduce infrastructure costs;
2. Reduce future development costs;
3. Reduce maintenance costs;
4. Ensure interoperability;
5. Enhance user experience with single sign-on and federated credential support;
6. Reduce authentication system development and acquisition costs.

4. Duplication of Efforts

The information collection requirements are not duplicated through any other effort.

The collection of this additional information will enable IDM to create a single identity credential to replace multiple credentials (i.e., usernames and passwords). This credential will be:

- Interoperable with digital identity credentials used by other organizations;
- Linked to an actual, vetted individual identity;
- Legally-binding and non-reputable;
- Scalable and will reduce the need for duplicate identity and access management efforts to support current/future legislatively mandated programs.

5. Small Businesses

There will be minimal impact on small businesses as the length of time to read, complete, and submit the online form is expected to take an average of twenty (20) minutes.

6. Less Frequent Collection

If this information is not collected, IDM will be unable to register an individual, issue credentials, identity proof in accordance with NIST standards, or authorize end-user access to CMS business applications and/or systems. Additionally, less frequent collections would result in unrealized cost and burden changes, and a failure to meet federally mandated security standards and requirements.

7. Special Circumstances

No special circumstances have been identified.

8. Federal Register/Outside Consultation

The 60-day notice published in the Federal Register on 3/19/2021 (86 FR 14926).
No comments were received.

The 30-day notice published in the Federal Register on 6/1/2021 (86 FR 29264).

9. Payments/Gifts to Respondents

There are no payments or gifts to respondents.

10. Confidentiality

IDM is covered under the System of Records Notice titled, "Individuals Authorized Access to Centers for Medicare & Medicaid Services Computer Services (IACS), HHS/CMS/OIS," SORN 09-70-0538. Publication date: 11/13/2007.

The information collected will be gathered and used solely by CMS and approved contractor(s). Information confidentiality will conform to HIPAA and FISMA requirements. Respondents may also access CMS Terms of Service and CMS Privacy Statement on the CMS.gov website.

11. Sensitive Questions

There are no questions regarding sexual preference, religion, or medical history.

IDM will collect the full 9-digit SSN. Collecting the full SSN during identity proofing is necessary in order to verify that the *asserted* identity corresponds to a *real* individual and to comply with NIST 800-63 guidance. Executive Order 9397, as amended by Executive Order 13478, permits Federal agencies to utilize individuals' SSNs when necessary even if CMS does not have specific program authority to collect SSNs. The Executive Order (with amended text – bolded and struck) is listed below.

Section 1. Policy **It is the policy of the United States that Federal agencies should conduct agency activities that involve personal identifiers in a manner consistent with protection of such identifiers against unlawful use.**

WHEREAS certain Federal agencies from time to time require in the administration of their activities a system of numerical identification of accounts of individual persons; and WHEREAS some seventy million persons have heretofore been assigned account numbers pursuant to the Social Security Act; and

WHEREAS a large percentage of Federal employees have already been assigned account numbers pursuant to the Social Security Act; and
WHEREAS it is desirable in the interest of economy and orderly administration that the Federal Government move towards the use of a single unduplicated numerical identification system of accounts and avoid the unnecessary establishment of additional systems: NOW, THEREFORE, by virtue of the authority vested in me as President of the United States, it is hereby ordered as follows:

1. Hereafter any Federal department, establishment, or agency may**,** whenever the head thereof finds it advisable to establish a new system of permanent account numbers pertaining to individual persons, utilize the Social Security Act account numbers assigned pursuant to title 20, section 422.103 of the Code of Federal Regulations and pursuant to paragraph 2 of this order.
2. The Social Security Administration shall provide for the assignment of an account number to each person who is required by any Federal agency to have such a number but who has not previously been assigned such number by the Administration. The Administration may accomplish this purpose by (a) assigning such numbers to individual persons, (b) assigning blocks of numbers to Federal agencies for reassignment to individual persons, or (c) making such other arrangements for the assignment of numbers as it may deem appropriate.
3. The Social Security Administration shall furnish, upon request of any Federal agency utilizing the numerical identification system of accounts provided for in this order, the account number pertaining to any person with whom such agency has an account or the name and other identifying data pertaining to any account number of any such person.
4. The Social Security Administration and each Federal agency shall maintain the confidential character of information relating to individual persons obtained pursuant to the provisions of this order.
5. There shall be transferred to the Social Security Administration, from time to time, such amounts as the Director of the Office of Management and Budget (OMB**)** shall determine to be required for reimbursement by any Federal agency for the services rendered by the Administration pursuant to the provisions of this order.
6. This order shall be implemented in accordance with applicable law and subject to the availability of appropriations.
7. This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies, instrumentalities, or entities, its officers, employees, or agents, or any other person;
8. This order shall be published in the FEDERAL REGISTER.

To achieve NIST assurance level 3 (AL-3), which is required for access to most CMS systems, financially-based questions must be used. During the identity proofing process, the individual will be asked to answer financially-based multiple choice questions that are generated using the information entered by the user. Per the Fair Credit Reporting Act (FCRA), the user will see a disclaimer that explains the access of credit report data. The user will need to check the box to continue the process. This type of query does not affect their credit score and no financial data is stored by IDM.

SSN (and all PII data) is protected as described below:

- Data Collection and In-Transit:
  - All communications will be via Hypertext Transfer Protocol Secure (HTTPS) connection, port 443 and 2048 certificates with 256-bit encryption for the tunnel. Screens will have input masking ability for SSN. Users will have to provide the last 4 digits of their SSN or Date of Birth (DOB) and other attributes to establish identity for Help Desk calls and Help Desk agents will have to login to IDM with multi-factor authentication (MFA) to access user information. CMS web-service calls made to Experian's Precise ID℠ use/support Transport Layer Security (TLS) V1.0 or higher are in line with FIPS 140-2 compliance using hardware / software solutions (Datapower XG45 with Hardware Security Module (HSM)). IDM data will be sent to Secure Lightweight Directory Access Protocol (LDAPS) and Java Database Connectivity (JDBC) over Secure Socket Layer (SSL).
- Data Storage:
  - Experian Precise ID℠ inquiry data is stored in a DB2 mainframe database and is appropriately protected using layers of network, application, physical, and administrative controls rather than encryption (due to the volume of data processed / performance reasons). Experian's compensating controls in lieu of data at rest encryption are accepted by Qualified Security Assessor (QSA) for the Payment Card Industry Data Security Standard (PCI DSS) compliance process. CMS inquiry data resides only on Experian's internal network (DB2 on a mainframe) segregated from other client data, behind three layers of firewalls and network intrusion detection equipment that is monitored constantly by a Global Security Operations Center (GSOC). Network equipment and servers housing the solution must pass a vulnerability assessment before being put into production and periodic scans/assessments thereafter. Precise ID℠ is part of Experian's Application Certification Program and is housed only in Experian's secure data center. Experian enforces full disk encryption on all workstations and removable media using FIPS 140-2 certified products. Because Experian has redundant data centers, there is no need to back up CMS information.
  - IDM will store the full SSN in Okta and in the IDM Hub using FIPS 140-2compliant encryption algorithm and key management.
- Archive:
  - Experian Precise ID℠ data is kept for a minimum of seven (7) years and is archived to tapes stored onsite at the data center, which is a Tier Level 4 security facility (Maximum security). The tapes never leave the facility and are accessed

using an automated robotic system, which enforces user authentication and authorization.

  - CMS will retain archived information pursuant to the Records Management Schedule developed for IDM. The disposition authority for IDM Master Files are identified below:

    1. Registration files - Disposition Authority, GRS 24, Item 13a1
    2. Authorization files - Disposition Authority, GRS 24, Item 13a1
    3. ID Management files - Disposition Authority: GRS 20, Item 1 4. Access Management files - Disposition Authority: GRS 20, Item 1

- Enterprise Infrastructure for IDM:
  - IDM is hosted at Amazon Web Services (AWS), which is a Federal Risk and Authorization Management Program (FedRAMP)-compliant, cloud-based infrastructure. AWS satisfies all of the essential characteristics of a Platform as a Service (PaaS), including broad network access and resource pooling. The IDM solution is designed to be a loosely coupled service-based and secure system that supports a high level of availability, scalability, and performance with implementation of multiple availability zones.
  - CMS has accredited the General Support System as compliant with FISMA.

12. Burden Estimates (Hours & Wages)

The average response time to complete the information collection is estimated to be 20 minutes per response, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection, with all respondents to reply electronically. Due to the individual differences of each collection—particularly, any online activity that may involve initial end-user account registration, recertification, or profile updates—the range of time for an end-user to complete data entry on the registration form(s) may vary between 5 to 20 minutes. Responses should certainly not require over 30 minutes from respondents. It is estimated that 560,000 users per year respond to the information collection requirement. In transitioning from EIDM to IDM, we also estimate that the total burden for end-user account registration to be 186,667 hours annually (560,000 respondents x 20min. per response / 60 min.). The time estimated for preparation and completion of the IDM data entry activities (i.e., end-user account registration, recertification, or profile updates) on the CMS Portal and IDM websites are based upon the professional judgment of staff members at the Centers for Medicare and Medicaid Services.

We believe that roughly 90% of users who respond to the information collection requirements can be categorized as office and administrative support, while the remaining 10% of users are physicians. Based on the most recent Bureau of Labor and Statistics Occupational and Employment Data May 2019 for Category 43-0000 (Office and Administrative Support

Occupations), the mean hourly wage for an administrative staff is $21.22, and for Category 290000 (Healthcare Practitioners and Technical Occupations), the mean hourly wage for a healthcare practitioner is $43.07. We have added 100% of the mean hourly wage to account for fringe and overhead benefits, which calculates to $86.08 ($43.07 + $43.07) for healthcare practitioners and $42.44 ($21.22 + $21.22) for administrative staff. The total weighted average is $46.80 ($86.08. x .10 + $42.44 x .90). We estimate the total annual cost to be $8,736,015 (186,667 hours x $46.80/ hour).

13. Capital Costs

There are no capital costs to the respondents.

14. Cost to Federal Government

The yearly average cost to the Government to support the IDM solution is estimated at $19.4M (million), which includes the following five (5) contracts: $2.5M for IDM Operations and Maintenance (O&M) and continuous modernization (CI/CD), including post-migration services; $7M for Okta licenses and professional services; $1.5M for IDM Help Desk services (BOSC); $6.6M for Experian Remote Identity Proofing (RIDP) services; and $1.8M for Cloud Computing Services-Amazon Web Services/Information Technology Operations (CCS-AWS/ITOps) Hub Hosting. These costs are anticipated to decrease in the out-years as the IDM system matures and as specific services (e.g., professional services, application migration support, contractor transition-out, etc.) are no longer needed to support and maintain the IDM solution.

15. Changes to Burden

In transitioning from EIDM to IDM, we estimate the total burden for end-user account registration in IDM to be 186,667 hours annually (560,000 respondents x 20 min. per response / 60 min.). As a result of inflation, there is a marginal increase to the annual cost burden compared to estimates provided in the last PRA submission. This adjustment is primarily due to an increase in the mean hourly wages of our anticipated users mentioned in *Section 12. Burden Estimates (Hours & Wages)* above. Based on the most recent Bureau of Labor and Statistics Occupational and Employment Data May 2019 (last modified on 3/31/2020) for Category 43-0000 (Office and Administrative Support Occupations), the mean hourly wage for an administrative staff increased from $19.93 to $21.22, and for Category 29-0000 (Healthcare Practitioners and Technical Occupations), the mean hourly wage for a healthcare practitioner increased from $42.55 to $43.07. This has caused an overall total annual cost increase of 5.45%, from $8,284,281 to $8,736,015.

16. Publication/Tabulation Dates

No publication or tabulation of data expected.

17. Expiration Date

The approved OMB Control No. (0938-1236) for this package is listed on the CMS Enterprise Portal and IDM Terms and Conditions websites, with an expiration date of 3/31/2021.

18. Certification Statement

This ICR does not contain surveys, censuses, or employ statistical methods; is not intended to be a Privacy Impact Assessment (PIA) required by the E-Government Act of 2002; and is not related to the Dodd-Frank Act (Dodd-Frank Wall Street Reform and Consumer Protection Act, P.L. 111-203), as referenced in the certification statement identified in Item 19, "Certification for Paperwork Reduction Act Submissions," of OMB Form 83-I. However, this ICR is related to the American Recovery and Reinvestment Act of 2009 (ARRA) and the Affordable Care Act [PPACA, P.L. 111-148 & 111-152] (Healthcare Reform), as described in Section A of this document.