US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

12/16/2025

OPDIV:

CMS

Name:

Multidimensional Insurance Data Analytics System

PIA Unique Identifier:

P-5961755-385901

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Contractor

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

N/A

Describe the purpose of the system.

The Multidimensional Insurance Data Analytics System (MIDAS) solution provides mission-critical functionality that Centers for Medicare & Medicaid Services (CMS) requires to implement and manage many provisions of the Affordable Care Act (ACA). To complete and sustain the various tasks mandated by the law, CMS created an analytics system that can support and inform these enterprise functions. This includes a data repository and analytics solution for capturing, aggregating, and analyzing health insurance and related information to support improved decision making, improved business processes and improved services to consumers, states, issuers, and other stakeholders.

MIDAS provides the following high-level functions:

Integrates data from multiple internal operational source systems into a single data store
Provides access to standardized reporting, ad hoc queries, and data visualization
Provides tools to allow data analysts to work directly with the data in the system to create custom reports, dashboards, and analytics
Provides operational reporting on the data collected and maintained

Additionally, MIDAS supports operational functions needed by CMS to manage ACA-related processes. MIDAS supports these processes through the following mechanisms:

Ingesting data from external stakeholders including issuers and State-based Marketplaces
Providing detailed data extracts of data in MIDAS to other CMS systems or processes to support operations

Describe the type of information the system will collect, maintain (store), or share.

MIDAS does not collect or store user credentials. Authentication and authorization for MIDAS admins and end users is provided by Microsoft Active Directory Domain Services which is controlled by the CMS Cloud Computing Services (CCS) Team's Amazon Web Services (AWS) cloud. The CMS AWS Cloud general support system (GSS). The CMS AWS Cloud is covered by a separate PIA.

All data in MIDAS originates from other internal or external operational systems supporting the Affordable Care Act (ACA). MIDAS ingest data from these upstream systems.

Financial Management (FM)
Data Services Hub (DSH)
Health Insurance Oversight System (HIOS)
Health Insurance Casework System (HICS)
State-based Marketplaces (SBM)
Federally Facilitated (FF)
Enrollment Baseline Data (EBD)
Logistics Management Institute (LMI)
Electronic Data Interchange (EDI)
National Insurance Producer Registry (NIPR)
EDGE Recal (FFM)
EDGE Recal (RTI)
OPERA (OA)
INCON
Center for Program Integrity CPI (Reli Group)
Duty First (DFC)
ISSUERS

MIDAS has data from multiple ACA-related systems at Centers for Medicare & Medicaid Services (CMS) and data from external partners including issuers and state-based Marketplaces. The data contained in MIDAS includes:

Consumer eligibility and enrollment data (includes names, addresses, email, phone, date of birth, Social Security Number (SSN), Passport number, and employment status)
Issuer Plan Management data
Consumer system account data (includes name and email address)
Issuer Vendor Management data

Data in MIDAS is maintained indefinitely at this time. DAA-GRS-2013-0007-0013 advises to

delete/destroy Personally Identifiable Information (PII) data when business use ceases.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

The data contained in MIDAS supports the following functions:

Consumer Assistance (45 CFR 155.205), Navigator Program (45 CFR 155.210), Agent Broker program (45 CFR 155.220): Data may support Centers for Medicare & Medicaid Services (CMS) certification of individuals assisting qualified individuals, employees and enrollees to enroll in Qualified Health Plans (QHP) through the Exchange. These individuals are required to register with an Exchange prior to providing any assistance.

Qualified Health Plan (QHP) certification (45 CFR 155.1000): Issuers are required to report contact information and business identifying information of QHPs seeking certification, as well as other information necessary to administer and evaluate the program.

Eligibility Determinations (45 CFR 155. 300, 155.305, 155.310), Eligibility Appeals (45 CFR 155.355) Exemption Determinations (45 CFR 155.605): Data may support eligibility determinations, eligibility appeals, and exemption determinations for any applicant/enrollee who applies or appeals, or on whose behalf an application is filed. Data also may support disclosure of information to another Federal agency, agency of a State government, a non-profit entity operating an Exchange for a State, an agency established by State law, or its fiscal agent about applicants to obtain information that help CMS, pursuant to agreements with CMS, to determine the eligibility of applicants to enroll in QHPs through an Exchange, in insurance affordability programs, or for a certification of exemption from the individual responsibility requirement.

Submission of Notices (45 CFR 155.230): Data may be used to support issuance of notices.

Premium Payment (45 CFR 155.240): Data may support the Exchange notification to QHP Issuers of premium payment due from enrollees.

Small Business Health Opportunity Program (SHOP) (Subpart H): Data may support information necessary for determining eligibility and enrolling qualified employees in SHOP and stores SHOP employer records.

Enrollment in QHPs (45 CFR 155.400): Data may support determination of eligibility for enrollment in QHPs and storage of enrollment records.

Oversight and Financial Integrity (45 CFR 155.200(c)): Data may be used to fulfill the Federally-facilitated Exchange's (FFE) responsibility for performing oversight functions with respect to issuer compliance with market-wide and Exchange specific standards in connection with QHPs certified by the FFE.

Administration of Advance Premium Tax Credits (APTC) and Cost Sharing Reductions (CSR) (45 CFR 155.340): Data may be used to support advance payments made to issuers monthly for APTC and CSR for eligible enrollees, and information about cost-sharing payments necessary to reconcile estimates of cost-sharing reductions with actual cost-sharing reductions.

Coordination with Medicaid, Children's Health Insurance Program (CHIP), Basic Health Plan (BHP) and Pre-Existing Conditions Insurance Plan (PCIP) (45 CFR 155.345): Data may be used to support determinations of eligibility.

Only authorized users can access/retrieve MIDAS data. They need to be connected to the CMS

virtual private network (VPN) and sign in with their Enterprise User Administration (EUA) credentials before accessing the data.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Social Security Number
Date of Birth
Name
E-Mail Address
Mailing Address
Phone Numbers
Employment Status
Passport Number
-- Consumer eligibility and enrollment data (includes all the above and addresses)
-- Issuer Plan Management data
-- Consumer system account data (includes name and email address)
-- Issuer Vendor Management data
No Federal Tax Information (FTI) is contained in MIDAS. FTI is used in the Federal and State-based Exchanges but MIDAS does not receive FTI from these systems. MIDAS receives other data from these systems but specifically excludes FTI.

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees
Public Citizens
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors
Public Citizen data collected is from Consumers in Health Insurance Marketplaces.
Business partner data collected is from Health Insurance issuers.

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

MIDAS serves as the central hub for analyzing the data collected within the marketplace systems. As such the data is used for a variety of needs to ensure the integrity of the program, provide for operational data needs (e.g. certifications, notices, etc.), and accessibility of the system (regarding eligibility requirements and assistance). The PII that is processed and stored in MIDAS is used for other operational functions of the exchange. This use is for performing functions such as the appeals process, tax credit administration, and premium payment information.

Describe the secondary uses for which the PII will be used.

Internal Centers for Medicare & Medicaid Services (CMS) and HHS data analysts have access to this data to support analytics, reporting, research and surveys.

Identify legal authorities governing information use and disclosure specific to the system and program.

The ACA (1411(g)) permits the use and disclosure of PII collected or created by an Exchange to ensure the efficient operation of the Exchange. 45 CFR 155.260.

1. Consumer Assistance (45 CFR 155.205)

2. Navigator Program (45 CFR 155.210)
3. Agent Broker program (45 CFR 155.220)
4. Qualified Health Plan (QHP) certification (45 CFR 155.1000)
5. Eligibility Appeals (45 CFR 155.355)
6. Submission of Notices (45 CFR 155.230)
7. Premium Payment (45 CFR 155.240)
8. Small Business Health Opportunity Program (SHOP) (Subpart H)
9. Exemption Determinations (45 CFR 155.605)
10. Enrollment in QHPs (45 CFR 155.400)
11. Eligibility Determinations (45 CFR 155. 300, 155.305, 155.310)
12. Oversight and Financial Integrity (45 CFR 155.200(c))
13. Establishment of Exchange network adequacy standards (45 CFR 155.1050)
14. Quality Assessments, Disclosures & Data Reporting (45 CFR 155.200(d))
15. Administration of Advance Premium Tax Credits (APTC) and Cost Sharing Reductions (CSR) (45 CFR 155.340)
16. Coordination with Medicaid, Children's Health Insurance Program (CHIP), Basic Health Plan (BHP) and Pre-Existing Conditions Insurance Plan (PCIP) (45 CFR 155.345)

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

HIX 09-70-0560 February 6, 2013

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Other
Government Sources
Within the OPDIV
Other Federal Entities
Non-Governmental Sources
Public

Identify the OMB information collection approval number and expiration date

OMB No. 0938-1156, expiration date: 09/30/2027

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

Computer Matching Agreements (CMAs)
2016-08 (CMA btw. Centers for Medicare & Medicaid Services (CMS) and Veterans Health Administration)
2016-02 (CMA btw. CMS and US Dept of Defense)
2018-09 (CMA btw. CMS and Internal Revenue Service) [a work in progress]

2018-09 (CMA btw. CMS and US Dept of Homeland Security) [a work in progress]
2016-11 (CMA btw. CMS and State-based Exchanges)
2016-09 (CMA btw. CMS and Social Security Administration)
2016-14 (CMA btw. CMS and Office of Personnel Management)
2016-15 (CMS btw. CMS and Peace Corps)

Information Exchange Agreements (IEAs)
2013-01 (IEA btw. CMS and Internal Revenue Service)
2013-02 (IEA btw. CMS and State-based Exchanges)
2013-03 (IEA btw. CMS and State Medicaid/Children's Health Insurance Program (CHIP) Agencies)

Describe the procedures for accounting for disclosures.

Disclosures are tracked through a workflow-management tool maintained at Centers for Medicare & Medicaid Services (CMS). Requests to disclose personally identifiable information (PII) are tracked in this system to maintain the date of the request, the requestor, the recipient of the disclosure, and the date the disclosure was made. Copies of output files containing the disclosed information are maintained securely within the MIDAS platform. Data Use Agreement #25792.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

The PII contained in MIDAS is collected from other source systems. The source systems identified in the System of Record and Notice (SORN) have the responsibility to notify individuals.

HIX 09-70-0560 February 6, 2013
HIX 09-70-0560 May 27, 2013
HIX 09-70-0560 October 23, 2013

HIX 09-70-0560 February 14, 2018

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

Participation in the Health Insurance Marketplace by a consumer is voluntary. Consumers that have existing health insurance are not required to participate in the Federal or State Marketplaces. Consumers without insurance can purchase insurance through the Federal or State Marketplaces, through private exchanges, through agents or brokers, directly with health insurance issuers, or choose not to purchase insurance (they may be subject to a tax penalty under this scenario).

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

The PII contained in MIDAS is collected from other source systems. The source systems identified in the System of Record and Notice (SORN) have the responsibility to notify individuals.

All major system changes concerning personally identifiable information (PII) are published for comment in the Federal Register as part of a modification of the applicable SORN.

HIX 09-70-0560 February 6, 2013
HIX 09-70-0560 May 27, 2013
HIX 09-70-0560 October 23, 2013

HIX 09-70-0560 February 14, 2018
Edit comment

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

An individual record subject who wishes to know if MIDAS system contains records about him or her should write to the system manager who will require the system name, and for verification purposes, the subject individual's name (woman's maiden name, if applicable), and social security number (SSN) (furnishing the SSN is voluntary, but it may make searching for a record easier and prevent delay).

An individual seeking access to records about him or her in this system should write to the system manager and reasonably specify the record contents being sought. (These procedures are in accordance with Department regulation 45 CFR 5b.5(a)(2).)

To contest a record, the subject individual should contact the system manager and reasonably identify the record and specify the information being contested. The individual should state the corrective action sought and the reasons for the
correction with supporting justification. (These procedures are in accordance with Department regulation 45 CFR 5b.7.)

System Manager:
Director, Consumer Information and Insurance Systems Group, Center for Consumer Information and Insurance Oversight, Centers for Medicare & Medicaid Services
7501 Wisconsin Ave, 9th Floor
Bethesda, MD 20814

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

MIDAS performs reconciliations with the upstream systems that provide data to MIDAS to ensure that the data in MIDAS aligns with the data in these upstream systems. Overall records count, as well as aggregated sums of key business values and comparison of data keys are used to verify that data in MIDAS matches the source system. Additionally, data reports created in MIDAS are compared to data reports from source systems to ensure accuracy, integrity, and alignment of data in MIDAS.

Identify who will have access to the PII in the system and the reason why they require access.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

MIDAS applies the principle of least privilege as well as a role-based view on granting rights. All access for the groups listed here is requested and approved before being granted. All Production access requires Program Manager approval.
Each user is assigned a Role, and each Role's rights are restricted to only the data and server resources needed to perform their job. Access requests are tracked via service request tickets. For planning, approval, and auditing, MIDAS utilizes a Roles and Responsibilities matrix to review and track what resources are accessible at the application level as well as the server level. A monthly audit is performed for system accounts and biweekly audit of user accounts is required.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

For planning, approval, and auditing, MIDAS utilizes a Roles and Responsibilities matrix to review and track what resources are accessible at the application level as well as the server level. Administrators only grant access to servers needed for their role and only assign users to the appropriate access groups required to perform their job function. Application users must be granted rights to each data set individually; at the MIDAS application level there is no single role that may access all data.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

Annual security, Ethics, and Business Conduct Training is provided.
Annual Centers for Medicare & Medicaid Services (CMS) Annual Security and Privacy Awareness Training (CBT) is required anyone who access a CMS system.
MIDAS specific data use agreements (DUA) for all project team members (signed/filed) detail some responsibilities expected when handling sensitive data.
MIDAS specific security training is conducted by the System Security Officer and Information System Security Officer that consists of specific CMS Acceptable Risk Safeguards (ARS) security and privacy controls that adhere to the CMS policies and is tracked by the MIDAS team per CMS Security policy.

Describe training system users receive (above and beyond general security and privacy awareness training).

System users receive functional training via webinars and presentations when new users are added to the program, and after significant functionality changes occur.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

Data in MIDAS is maintained indefinitely. DAA-GRS-2013-0007-0013 advises to delete/destroy PII data when business use ceases.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

MIDAS applies the principle of least privilege as well as a role-based view on granting rights. All access for the groups is requested and approved before being granted. All Production access requires Program Manager approval.
Each user is assigned a Role, and each Role's rights are restricted to only the data and server resources needed to perform their job. Access requests are tracked via service request tickets. For planning, approval, and auditing, MIDAS utilizes a Roles and Responsibilities matrix to review and track what resources are accessible at the application level as well as the server level. A monthly audit is performed for system accounts and biweekly audit of user accounts is required. New MIDAS project team members are processed through an on-boarding process that defines their role and all information and approvals are archived in a trackable service request.

MIDAS is hosted in a secure, Federal Information Security Management Act (FISMA)-compliant data center and the Federal Risk and Authorization Management Program (FedRAMP) approved cloud. Physical access to the system is limited to data center administrators only. User access is also dependent upon Centers for Medicare & Medicaid Services (CMS) approval.