Status: Final

Form Date: 15-JAN-15

Question 1: OPDIV
Question 1 Answer: CMS

Question 2: PIA Unique Identifier (UID):
Question 2 Answer: P-5961755-385901

Question 2A: Name:
Question 2A Answer: Multidimensional Insurance Data Analytics System

Question 3: Which of the following objects does this PIA Cover?
Question 3 Answer: Major Application

Question 3A: Identify the Enterprise Life-Cycle Phase of the System:
Question 3A Answer: Operations and Maintenance

Question 3B: Is this a FISMA Reportable System?
Question 3B Answer: Yes

Question 4: Does the system include a publicly available Web interface?
Question 4 Answer: No

Question 5: Identify the operator
Question 5 Answer: Contractor

Question 7: Is this a new or existing system
Question 7 Answer: Existing

Question 8: Does the system have Security Authorization (SA)?
Question 8 Answer: Yes

Question 8A: Date of Security Authorization
Question 8A Answer: 11-JUL-13

Question 8B-1: Planned date of Security Authorization - Not Applicable
Question 8B-1 Answer: Checked True

Question 8C: Breifly explain why security authorization is not required
Question 8C Answer: MIDAS has a current Authority to Operate (ATO) which should satisfy this requirement which expires 06/30/16

Question 9 : Indicate the following reason(s) for updating this PIA.
Choose from the following options.
PIA Validation (PIA Refresh/Annual Review): Checked
Significant System Management Change: Checked
Conversion: Checked
New Interagency Uses: Checked
Internal Flow or Collection: Checked
Other...: Changes in usage of the data within the system

Question 10: Describe in further detail any changes to the system that have occurred since the last PIA.
Question 10 Answer: The original purpose of MIDAS was to provide reporting and analytical capabilities of

key Affordable Care Act-related data to Centers for Medicare & Medicaid Services (CMS) and other stakeholders. Recent program needs have required that data in MIDAS also be used to support Marketplace-related operational processes, which has changed how the data in MIDAS is being used and created a need to ingest data from new sources to support these operational processes.

Question 11: Describe the purpose of the system.
Question 11 Answer: The MIDAS solution will provide mission-critical functionality that Centers for Medicare & Medicaid Services (CMS) requires to implement and manage many provisions of the Affordable Care Act (ACA). In order to complete and sustain the various tasks mandated by the law, CMS must create an analytics system that is capable of supporting and informing 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

Question 12: Describe the type of information the system will collect, maintain (store), or share. (Subsequent questions will identify if this information is PII and ask about the specific data elements.)
Question 12 Answer: 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.

Federally-Facilitated Marketplace (FFM)
Data Services Hub (DSH)
Health Insurance Oversight System (HIOS)
Health Insurance Casework System (HICS)
State-based Marketplaces (SBM)
Issuer enrollment systems
Integrated Marketplace Access System (IMAS)
Small Business Health Opportunity Program (SHOP)
Enrollment & Payment Store (EPS)
External Data Gathering Environment (EDGE)

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), and consumer-provided income information)
-- Issuer Plan Management data
-- Consumer system account data (includes name and email address)
-- Issuer Vendor Management data (includes financial account information)

Question 13: Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

Question 13 Answer: 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 in order 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 on a monthly basis 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.

Question 14: Does the system collect, maintain, use, or share PII?
Question 14 Answer: Yes

Question 15 : Indicate the type of PII that the system will collect or maintain.
Indicate the type of PII the system will collect or maintain.
Social Security Number: Checked True
Date of Birth: Checked True
Name: Checked True
Mother's Maiden Name: Not Checked
Mailing Address: Checked True
Phone Numbers: Checked True
Financial Accounts Info: Checked True
Education Records: Not Checked
Military Status: Checked True
Employment Status: Checked True
Passport Number: Checked True
Taxpayer ID: Checked True
Q15 Other 1: 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.

Question 16 : Q6

Indicate the categories of individuals about whom PII is collected, maintained, or shared.
Employees: Checked True
Public Citizens: Checked True
Business Partner/Contacts (Federal/state/local agencies: Checked True
Vendor/Suppliers/Contractors: Checked True
Q16 Other: Public Citizen data collected is from Consumers in Health Insurance Marketplaces

Business partner data collected is of Health Insurance issuers

Question 17: How many individuals' PII is in the system?
Question 17 Answer: 1,000,000 or more

Question 18: For what purpose is PII used?
Question 18 Answer: 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)

Question 19: Describe secondary uses for which PII will be used (e.g. testing, training or research)
Question 19 Answer: Internal Centers for Medicare & Medicaid Services (CMS) data analysts have access to this data to support analytics, reporting, research and surveys.

Question 20: Describe the function of the SSN.
Question 20 Answer: The social security number (SSN) is not used directly in MIDAS, however the SSN can be included in detailed data extracts that MIDAS provides in support of operational processes. In these cases, the SSN is used in these processes to support consumer eligibility determinations, resolution of data inconsistencies, transfers of consumer accounts to state Medicaid agencies, and consumer outreach.

Question 20A: Describe the function of the SSN.
Question 20A Answer: Section 1414 of the Patient Protection and Affordable Care Act (ACA)

The ACA (1411(g)) permits the use and disclosure of personally-identifiable information (PII) collected or created by an Exchange to ensure the efficient operation of the Exchange. 45 CFR 155.260 was originally drafted with the understanding that Exchange minimum functions would ensure the efficient operation of the Exchange. Later it became clear that there were additional uses and disclosures that would not necessarily fit into the Exchange minimum function but ensured the efficient operation of an Exchange so the new version of the regulation permits the Secretary of the Department of Health and Human Services (DHHS) to determine that the disclosure of PII for purposes other than Exchange minimum functions can be made as long as certain substantive and procedural steps are followed and the consent of the subject individuals is obtained.

Question 21: Describe secondary uses for which PII will be used (e.g. testing, training or research)

Question 21 Answer: 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)

Question 22: Describe secondary uses for which PII will be used (e.g. testing, training or research)
Question 22 Answer: Yes

Question 22A-1B: SORN #1
Question 22A-1B Answer: HIX 09-70-0560 October 23, 2013

Question 22A-2B: SORN #2
Question 22A-2B Answer: HIX 09-70-0560 May 27, 2013

Question 22A-3B: SORN #3
Question 22A-3B Answer: HIX 09-70-0560 February 6, 2013

Question 22A-4: In Progress?
Question 22A-4 Answer: Checked True

Question 23A: Identify the OMB information collection approval number and expiration date
Question 23A Answer: OMB No. 0938-1191, expiration date: 04/30/2016

Question 23 : Identify the sources of PII in the system.
Hard Copy: Mail/Fax: Checked True
Online: Checked True
Other: Checked True
Government Sources
Within the OPDIV: Not Checked
Other HHS OPDIV: Not Checked
State/Local/Tribal: Not Checked
Other Federal Entities: Checked True
Non-Government Sources
Members of the Public: Checked True
Other: Checked True

Question 24: Is the PII shared with other organizations?
Question 24 Answer: Yes

Question 24A : Identify with whom the PII is shared or disclosed and for what purpose.
Identify with whom the PII is shared or disclosed and for what prupose.
Within HHS: Checked True
Identify with whom the PII is shared or disclosed and for what prupose.
Within HHS: -- Support for Health Insurance Marketplace program related operational processes.
-- Oversight and financial integrity reporting and quality activities.
-- Office of the Assistant Secretary for Planning and Evaluation (HHS ASPE) - To support oversight an
OtherFed: Checked True
OtherFed: -- Veterans Health Administration - Consumer eligibility determinations for Marketplace coverage
-- US Dept of Defense - Consumer eligibility determinations for Marketplace coverage
-- US Dept of Homeland Security - Consumer eligibility determinations for
OtherFed: Checked True
OtherFed: --Transfer of consumer eligibility information to state Medicaid agencies
--Transfer of consumer eligibility and enrollment data to states transitioning from the Federal Marketplace to a State-based Marketplace
OtherFed: Checked True
OtherFed: Transfer of consumer insurance plan enrollment data to health insurance issuers to support consumer enrollment int health insurance coverage

Question 24B: Describe any agreements in place that autorizes the information sharing.
Question 24B Answer: Computer Matching Agreements (CMAs)
2013-06 (CMA btw. Centers for Medicare & Medicaid Services (CMS) and Veterans Health Administration)
2013-07 (CMA btw. CMS and US Dept of Defense)
2013-08 (CMA btw. CMS and Internal Revenue Service)
2013-10 (CMA btw. CMS and US Dept of Homeland Security)
2013-11 (CMA btw. CMS and State-based Exchanges)
2013-12 (CMA btw. CMS and Social Security Administration)
2014-14 (CMA btw. CMS and Office of Personnel Management) [a work in progress]
2014-15 (CMS btw. CMS and Peace Corps) [a work in progress]

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)

Question 24C: Describe any agreements in place that autorizes the information sharing.
Question 24C Answer: 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 in order 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.

Question 25: Describe the process in place to notify individuals that their personal information will be collected.
If no prior notice is given, explain the reason.
Question 25 Answer: HIX 09-70-0560 February 6, 2013
HIX 09-70-0560 May 27, 2013
HIX 09-70-0560 October 23, 2013

Question 26: Is the submission of PII by individuals voluntary or mandatory?
Question 26 Answer: Voluntary

Question 27: Describe the method for individuals to opt-out of collection or use of theri PII.
If there is no option to object to the information collection, provide a reason.

Question 27 Answer: 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).

Question 28: Describe the process to notify and maintain consent from the individuals whose PII is in the system.
Question 28 Answer: 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 System of Record (SOR).

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

Question 29: 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. If no process exists, explain
why no.
Question 29 Answer: An individual record subject who wishes to know if this 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

Question 30: Describe the process in place for periodic reviews of PII contained in the system to ensure the data's
integrity, availability, accuracy and relevancy. If no processes are in place, explain why not.
Question 30 Answer: 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 counts, 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.

Question 31 : Identify who will have access to the PII in the system and the reason why they require access.
Identify who will have access to the PII in the system and the reason why they require access.
User Check Box: Checked True
User Reason: Centers for Medicare & Medicaid Services (CMS) Data Analysts and designated contractor data analysts need access to this data to support reporting, analytics, and support for operational processes

Administrators Check Box: Checked True
Administrator Reason: Administrators are required in order to support system operations and maintenance
Developers Check Box: Checked True
Developers Reason: Development of detailed data extracts from MIDAS that are provided to other systems or operational processes to support overall Affordable Care Act (ACA)-related functions at Centers for Medicare & Medicaid Services (CMS)
Contractors Check Box: Checked True
Contractors Reason: MIDAS is a contractor-managed system. Contractors need access to the personally-identifiable information (PII) to support system operations and maintenance.
Others Check Box: Not Checked

Question 32: Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII
Question 32 Answer: 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, approving, 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 quarterly user driven validation of accounts is required.

Question 33: 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.
Question 33 Answer: For planning, approving, 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 grant access to only the servers needed for their role. Administrators will only associate a user to the access groups required to perform their job. Application users must be granted rights to each data set individually, at the MIDAS application level there is no one role that may access all data.

Question 34: 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.
Question 34 Answer: -- Annual security training and Ethics and Business Conduct Training is provided.
-- Centers for Medicare & Medicaid Services (CMS) Annual Security Awareness Training (CBT).
-- MIDAS specific data use agreements (DUA) for all team members (signed/filed) detail some responsibilities expected when handling sensitive data.
-- MIDAS specific security training conducted by System Security Officer and Information System Security Officer and that training consist of specific CMS Acceptable Risk Safeguards (ARS) 2.0 security controls that adhere to the CMS privacy controls and is tracked by the MIDAS team per CMS Security policy.

Question 35: Describe training system users receive (above and beyond general security and privacy awareness
training).
Question 35 Answer: Users receive functional training via webinars and presentations when new users are onboarded and after significant functionality changes.

Question 36: Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to
privacy provisions and practices.
Question 36 Answer: Yes

Question 37: Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite

specific records retention schedules.
Question 37 Answer: Data in MIDAS is maintained indefinitely at this time. Per System of Record Notice (SORN) 09-70-0560 "These records will be maintained until they become inactive, at which time they will be retired or destroyed in accordance with published records schedules of the Centers for Medicare & Medicaid Services as approved by the National Archives and Records Administration."

Question 38: Describe, briefly but with specificity, how the PII will be secured in the system using administrative,
technical, and physical controls.
Question 38 Answer: MIDAS applies the principle of least privilege as well as a role based view on granting rights. All access for the groups are 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, approving, 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 quarterly user driven validation of accounts is required. New MIDAS 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. 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 and is not accessible to users outside of CMS networks.