

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/05/2024

OPDIV:

CMS

Name:

CM - Novitas Solutions Inc

PIA Unique Identifier:

P-3922525-089901

The subject of this PIA is which of the following?

General Support System (GSS)

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?

Yes

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.

No changes have occurred.

Describe the purpose of the system.

The CM – Novitas Solutions Inc (CM-NSI) system is a collection of systems that are processed in the CM-NSI data center with the purpose of paying providers (doctors and hospitals) for their services. CM-NSI receives Medicare Fee-For-Service claims that originate with providers. The claims are validated as complete by CM-NSI, then the claims are loaded into one of the Fee-For-Service systems; the Fiscal Intermediary Standard System (FISS) for Medicare Part A claims, the Multi-Carrier System (MCS) for Medicare Part B claims and ViPS Medicare System (VMS) for Medicare Durable Medical Equipment claims, for processing. This processing occurs at the CMS Virtual Data Centers. Employees at CM-NSI access the FISS, MCS and VMS systems to adjudicate the claims in accordance with CMS policies and standards. Novitas Solutions manages the payment processing website on behalf of CMS, with a link to their privacy policy.

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

The information is collected, maintained, or disseminated for three groups:

Beneficiaries - This information includes name, date of birth, Medicare Beneficiary Identifier (MBI), health insurance claim number, mailing address, phone numbers, medical record numbers, medical notes, military status and/or records, employment status and or records, health insurer name/plan, health insurer group number, and patient marriage status for the purpose of processing and paying claims.

Providers - This information includes name, tax id, mailing address, phone numbers, financial account information and/or numbers, certificates, device identifiers, email address, for the purpose of processing and paying claims.

CM- Novitas Solutions Inc contractors and CMS employees - This information includes username, password, email address, name, social security number (SSN), driver's license number, education records, photographic identifiers, and employer or school name.

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

The CM – Novitas Solutions Inc (CM-NSI) system processes Medicare Fee-For-Service claims. Medicare beneficiary claims data processed was collected by providers at the time of service and includes information necessary to process Medicare Fee-For-Service claims. Data from providers is maintained to validate that the provider is registered to submit Medicare claims and registered to inquire about claim status. Finally, data regarding CM-NSI contractors and CMS employees is used to access the system. Information can be retrieved by the beneficiary's name, health insurance claim number, and assigned unique provider identification number.

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

Photographic Identifiers

Driver's License Number

E-Mail Address

Mailing Address

Phone Numbers

Medical Records Number

Medical Notes

Financial Accounts Info

Certificates

Education Records

Device Identifiers

Military Status

Employment Status

Taxpayer ID

Other: Employer or school name, Health Insurer Name/Plan, Health Insurer Group Number, Patient Marriage and Employment Status, Medicare Beneficiary Identifier (MBI), Health Insurance Claim Number, user credentials- user ID, name, password.

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

Employees
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors
Patients

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

Beneficiary PII is collected from patients to verify receipt of service and to properly pay claims. Provider PII is collected to verify the identity of the provider prior to gaining access to the CM – Novitas Solutions Inc (CM-NSI) web portal. Also, Novitas Solutions Inc. contractor and CMS employee PII is collected to verify the system user's identity and credentials.

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

N/A

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

Sections 1816, 1862 (b) and 1874 of Title XVIII of the Social Security Act (The Act) (42 United States Code (U.S.C.) 1395u, 1395y (b), and 1395kk)

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.

09-70-0501, "Medicare Multi-Carrier Claims System (MCS)"

09-70-0503, "Fiscal Intermediary Shared System (FISS)"

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person
Government Sources

Identify the OMB information collection approval number and expiration date

None
OMB 0938-017 Expires 12/31/2024

Public
Private Sector

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.

CMS determines how and with whom Medicare fee-for-service data is disclosed. As directed by CMS via contractual arrangements, the CM – Novitas Solutions Inc (CM-NSI) shares data with other CMS contractors for the purposes of fighting fraud, waste, and abuse. The CM-NSI contract requires that a Joint Operating Agreement to document the data that will be exchanged. These other contractors include, but are not limited to, Zone Program Integrity Contractors, Qualified Independent Contractors, and Quality Improvement Organizations.

Describe the procedures for accounting for disclosures.

Data that is shared with the CMS Virtual Data Centers to process Part A claims in the Fiscal Intermediary Standard System, Part B claims in the Multi-Carrier System, or ViPS Medicare System is tracked and accounted for through daily reporting and balancing routines. Data that is shared with other contractors designated by CMS is tracked and accounted for through case management software tools that are part of the collection of systems processed as part of the CM – Novitas Solutions Inc system. These other contractors include, but are not limited to, Zone Program Integrity Contractors, Qualified Independent Contractors, and Quality Improvement Organizations.

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

For the beneficiary, written notice is given when the beneficiary initially enrolls in the Medicare program and written or orally each time the beneficiary applies for service at a provider. For the provider, written notice is provided during enrollment for a website user id. For the CM-Novitas Solutions Inc. contractors and CMS employees, written notice is provided when they apply for a job.

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.

When a beneficiary's data is collected and sent to the CM - Novitas Solutions Inc (CM-NSI) system, the beneficiary has already agreed to share their information, so there is not an ability for them to opt out of PII data collection. A provider can opt out of providing PII to the CM-NSI system, but they will be denied access to the CM -NSI system for claims inquiry. The CM-NSI contractors and CMS employees cannot opt out of providing PII because the collection of the data is necessary for employment.

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

A System of Records Notice (SORN) was filed for the systems used to process provider claims. For Medicare Part A, the SORN is 09-70-0501 for the MCS. For Medicare Part B, the SORN is 09-70-0503 for the FISS. Due to the large number of beneficiaries and providers that would be impacted by a change, obtaining individual consent is not feasible. Therefore, in accordance with the Privacy Act, a new SORN would be published with a 60-day comment period to notify individuals of a change in use and/or disclosure of data by the CM - Novitas Solutions Inc system.

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.

Individuals are notified annually in the 'Medicare & You' handbook of their right to file a complaint if they believe their privacy rights have been violated. A phone number is included in the handbook and there is more information on www.medicare.gov. The phone number is 1-800-Medicare. When a beneficiary calls this number, they are contacting a CMS system known as the Next Generation Desktop (NGD), which is a system that is separate from the CM - Novitas Solutions Inc (CMS-NSI). To resolve complaints, CMS-NSI employees log onto the NGD system to retrieve and respond accordingly to complaints. The final resolution is managed and recorded in the NGD system.

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

The Medicare claims processing systems run by CM - Novitas Solutions Inc (CM-NSI) use the Common Working File (CWF) eligibility file and verification processes to ensure PII is timely, accurate and relevant. Integrity is maintained through system security and control processes that are reviewed by external auditors. Availability is maintained through system redundancies and CM-NSI is required to annually test disaster recovery capabilities. Relevancy and accuracy are maintained by the interactions with the shared systems (FISS, MCS, VMS) and CWF, which all have their own PIAs. These sources of the data from the shared system have their own processes to ensure the PII's accuracy and relevancy.

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.

Access to the systems is given based on need to know and job responsibilities to process Medicare claims using a user id and role-based access. Access is obtained using a CM - Novitas Solutions Inc access request form. The form must be approved by the designated approvers prior to access being granted.

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.

Access to the systems is controlled using security software. The user is given the least amount of access required to perform their job duties and is explicitly denied access by the security software unless otherwise granted.

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.

All CM-Novitas Solutions Inc. (CM-NSI) contractors and CMS employees are required to take annual training regarding the security and privacy requirements for protecting PII. In addition, role-based training is provided to individuals with significant access or security responsibilities. This annual role-based training is required by the CMS Chief Information Officer Directive 12-03. All training is modeled on and is consistent with training offered by the Department of Health and Human Services and CMS.

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

In addition to the general security and privacy awareness training, users must sign rules of behavior. Also, throughout the year, users are provided with newsletters, list serve messages and security bulletins to provide ongoing awareness of their security and privacy responsibilities.

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.

In accordance with the NARA RCS Job Number N1-440-04-003, records are maintained in a secure storage area with identifiers. Records are closed at the end of the fiscal year, in which paid, and

destroyed after 6 years and 3 months. All claims-related records are encompassed by the document preservation order and will be retained until notification is received from Department of Justice.

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

Access to the systems is given based on need to know and job responsibilities to process Medicare claims. CM - Novitas Solutions Inc (CM - NSI) maintainers use security software and procedural methods to provide "least privilege access" to grant or deny access to data based upon need to know. External audits also verify these controls are in place and functioning. Technical controls used include user identification, passwords, firewalls, virtual private networks, and intrusion detection systems. Physical controls used include guards, identification badges, key cards, cipher locks and closed-circuit televisions.

Identify the publicly-available URL:

www.novitas-solutions.com

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Does the website have any information or pages directed at children under the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

Yes

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

No