US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/20/2025

OPDIV:

CMS

Name:

CM - C2C Innovative Solutions Inc.

PIA Unique Identifier:

P-1946109-986856

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?

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.

No changes to support system. Completed annual review of Privacy Impact Assessment (PIA) content and review/update of contact information.

Describe the purpose of the system.

The purpose of this Center for Medicare (CM) C2C Innovative Solutions, Inc. (C2C) information system (CM-C2C) is to provide the platform to perform adjudication services for level 2 Medicare appeals of coverage determinations, payment disputes and the use of Durable Medical Equipment (DME). The adjudication services include processing appeal requests, tracking appeal data, and responding to correspondence related to the appeal.

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

The CM-C2C system collects and maintains information concerning Medicare beneficiaries, providers, and system users. The information on beneficiaries consists of name, address, date of birth, Health Insurance Claim Number (HICN), Medicare Beneficiary Identifier (MBI), correspondence

and medical records and notes, as well as assigned appeal number(s) and claim number(s), if applicable. Information about providers includes their name, office address, phone number and National Provider Identifier (NPI). Information about system users consists of names, usernames, and passwords.

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

The CM-C2C system obtains information concerning Medicare beneficiaries, providers, and system users from the Medicare Appeals System (MAS), another Centers for Medicare & Medicaid Services (CMS) information system which is also covered by a separate PIA. C2C staff retrieve records from MAS primarily using an appeal number, although they may need to query by beneficiary name or HICN/MBI number to find related appeal numbers. The records in MAS are Medicare beneficiary and medical service data related to appeals filed for Medicare service coverage or claim(s) payment information. MAS maintains its own PIA for the information collected, stored, and shared within it as the system of records.

The CM-C2C system is used by C2C in the performance of Medicare appeal services as a CMS Qualified Independent Contractor (QIC). C2C does not maintain or operate a system of records for CMS. QICs are responsible for conducting the second level of appeals of Medicare Part A, Part B, and DME coverage determinations, payment disputes and the use of DME. The adjudication services include processing appeal requests, tracking appeal data, and responding to correspondence related to the appeal, as set forth by Title II of the Medicare Prescription Drug, Improvement and Modernization Act of 2003 (MMA). C2C staff retrieve records from the CM-C2C system primarily using an appeal number, although they may need to query by beneficiary name or number to find related appeal numbers.

C2C and Texas Medical Foundation (TMF) are direct CMS contractors. Only authorized system users have access. Access includes authorized CMS contractors, C2C employees, C2C contractors and sub-contractors, and some vendors doing system development. To access the CM-C2C system, users provide their name, user identification (ID), and password to create a user account and obtain access to the system.

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

Yes

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

Date of Birth
Name
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Legal Documents
HICN/MBI, User ID, Password, NPI, Appeal Number, Claim Number and Payment information related to claim, Date of Death.

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

Employees
Public Citizens

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

Beneficiary and provider Personal Identifiable Information (PII) is used by C2C to prepare and route notification letters to appellants and complete the review of the appeal. System user PII is used to create and maintain the individually assigned credentials for system access.

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

None

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

Authority for information use and disclosure is given under Section 205 of Title II, Sections 1155 and 1156 of Title XI, Sections1812, 1814, 1816, 1842, 1869, and 1872 of Title XVIII of the Social Security Act as amended (42 United States Code Sections 405, 1320c-4, 1320c-5, 1395d, 1395f, 1395h, 1395u, 1395ff, and 1395ii). Additional authority is given under the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (Public Law 108-173).

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.

09-70-0566 Medicare Appeals System, published 12/16/2004 and updated 9/15/2006.

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Hardcopy

Email

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Other

Identify the OMB information collection approval number and expiration date

N/A

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.

We do not have any Memorandums of Understanding (MOUs) or Computer Matching Agreement.

We do have an Information Sharing Agreement (ISA) with CMS.

Describe the procedures for accounting for disclosures.

C2C only shares PII with authorized organizations, such as CMS and CMS contractors (Medicare Administrative Contractors (MACs), Quality Improvement Organizations (QIOs),

etc.).
C2C shares with authorized appellants with regards to QIC reconsideration appeal process. C2C also shares PII with beneficiaries or their authorized representatives regarding their specific beneficiary information.

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 source of the CM-C2C beneficiary personal information is the CMS operated MAS. MAS is covered by a System of Record Notice (SORN) (09-70-0566) and its own PIA. The CM-C2C system does not directly notify individuals that their personal information is being collected because the system uses personal information from the MAS system. Any required notifications are provided through MAS. Providers and beneficiaries are informed on their appeal request form that providing their information is voluntary but failure to provide all or part of the requested information may affect the determination of their appeal.

System users are notified as part of the employment process and to obtain access to the CM-C2C that their personal information is required.

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.

Beneficiary and provider PII is required for appeal processing and is received from the MAS system. MAS is covered by a SORN (09-70-0566) and its own PIA. If the appeals process requires individuals to verify the information in the MAS system, they are notified on the standardized processing letters that the information provided will be used to further document their appeal and that submission of the information requested is voluntary, but failure to provide all or any part of the requested information may affect the determination of the appeal.

System user credentials, PII, are mandatory for system access, so there is no option to opt-out.

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

The source of the CM-C2C beneficiary personal information is the CMS operated MAS. As a System of Record, MAS is covered by a SORN (09-70-0566) and its own PIA. MAS is responsible for the process to notify and obtain consent from individuals whose PII is in MAS when major changes occur to the system. Medicare beneficiaries and providers would find notification of any major changes to the MAS system, and affecting PII, through the updating or revision to the SORN in the Federal Register. Per the C2C website’s Privacy Statement, Beneficiaries may contact C2C by email (privacy@c2cinc.com).

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.

CM-C2C obtains PII from MAS. MAS PII is obtained from other systems which verify appellant PII. These systems include the Medicare Beneficiary Database (MBD), Health Plan Management System (HPMS), Next Generation Desktop (NGD) and National Plan and Provider Enumeration System (NPPES) which all are covered by their separate CMS PIAs. Contacts for these various applications are available from CMS.gov. If there are concerns about user PII, users can contact the MAS Help Desk.

If CM-C2C system users have concerns about their PII, they would contact the C2C IT help desk. The help desk would investigate the incident and provide direction to the user on if further action is necessary.

Edit comment

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 PII contained in the CM-C2C system is routinely backed up to ensure availability. PII is protected by encryption (at rest/in motion) to ensure confidentiality. For integrity, access controls are in-place and can only be modified by authorized system administrators. The beneficiary's PII is verified with the MAS for accuracy and relevancy at the time of appeal case creation and reviewed throughout the appeal process, maintaining the integrity of the PII. PII in claims processing is regularly reviewed for relevancy and accuracy.

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.

All system access requests are reviewed and approved by the appropriate business leadership prior access request submission. Supervisors must submit individuals access requests to C2C's IT management prior to account creation. For system use, C2C uses the principles of least privilege and need-to-know to grant access. The system has role-based access controls to ensure general and privileged users are only granted access commensurate with their assigned duties.

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.

The system uses the principle of least privilege as well as role-based access control to ensure system users are granted access on a "need-to-know" and "need-to-access" for performing their job functions.

System administrators review user accounts at least semi-annually. Any anomalies are addressed and resolved by contacting the user, and modifying their user data, or by removing their access if it is no longer required. Activities of all users including system administrators are logged and reviewed by the system Information Security staff to review system activities and access.

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 system users are required to complete the initial and quarterly Security and Privacy Awareness training. All personnel that will have access to CUI must complete the HHS role-based training. The training manager and privacy officers ensure that all personnel complete the required training. All security and privacy trainings are Computer Based Training (CBT) courses through our Learning Management System (LMS). Vendors with access are required to provide training attestations.

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

All C2C/TMF system users participate in monthly phishing testing campaigns. The information security department frequently distributes emails on security and privacy risks and threats, best practices, and recent attacks against the healthcare industry.

Privileged system users (admins, developers, and security personnel) commensurate with the

position they are working must also complete LMS role-based security and privacy training, continuity exercises/training, and security staff for incident response exercise/training.

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.

The CM-C2C system follows the CMS Records Schedule updated in September 2023. This includes the records retention policy for the MAS system. Data retention complies with the National Archives and Records Administration (NARA) Disposition Authority: N1-440-09-5 Item 1b, which states that records will be destroyed 10 years after cutoff or when no longer needed for CMS business. Per CMS, CM-C2C Medicare Claims Records are under a document destruction freeze. C2C is prohibited from destroying records for “Medicare Claims” and “Medicare Beneficiary Correspondence Files” per the CMS disposition instructions. Once the freeze is lifted, cutoff is at the close of the calendar year in which the contractor is paid. C2C will destroy 6-years and 3-months of records after cutoff.

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

The system’s management security and privacy controls consist of policies, procedures, and control standards. This is in addition to security and privacy training, role-based access permissions, and regular review of access logs and activities.

The system’s technical security controls consist of implementing security/privacy hardening (CIS Benchmarks) as the Active Directory (AD) Group Policy Objects (GPOs); restricting access using user ids, passwords, and two-factor authentication one-time passcode. Technical protection is also achieved through boundary controls, continuous monitoring for system usage and unexpected or malicious activity; the configuration of specialty hardware/software; in transit encryption; at rest encryption (full disk encryption of laptops, workstations, and backed-up snapshots).

The system’s physical security controls consist of restricted access areas (the company offices and data centers) are monitored and recorded. Only authorized personnel may access restricted areas with appropriate security permissions (access badge or issued door key). All external company office suite doors are controlled with badge access card readers. Designated limited restricted security areas are only accessible to approved personnel. Physical equipment and media are subject to documented handling procedures, including proper disclosure, disposal, and destruction as necessary. Environmental protections consist of protected cooling and power sources that are monitored.