US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/18/2025

OPDIV:

CMS

Name:

Unified Case Management Next Generation

PIA Unique Identifier:

P-6815589-583776

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

Significant System Management Change

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

The UCM application is undergoing a modernization using a bi-modal delivery model that will allow CPI to innovate and modernize UCM while sustaining current program commitments and release schedules. As part of this modernization, the application will incrementally migrate from the current Baltimore Data Center to the CMS AWS infrastructure, resulting in a shared or transitioning of inherited security controls that relate to the infrastructure and enterprise services.

The initial, January 2021, release included a new, minor functionality called the Compromised Number Record, and it is domiciled in the CMS AWS cloud infrastructure. The second major release, in May 2021, introduced Major Case Coordination (MCC), which refers to the process of selecting, preparing, prioritizing, organizing, and decision recording of high-profile cases as a result of the MCC Meetings. MCC in UCM NexGen provides the capability to streamline the overall MCC process, and

allow the user to select, schedule, prioritize, and record decisions in real-time and generate exports all within the UCM NexGen application. UCM NexGen provides users with a Medical Record Review (MRR) capability to initiate a Medical Review, track the progress of a Medical Review, complete and close-out a Medical Review, and summarize the findings of the Medical Review. Lead Management will allow users to initiate, assign, and prioritize cases based on correlated UCM data.

UCM will maintain connectivity to the CMS systems FPS and OnePI. UCM NexGen interfaces with these systems to retrieve financials, provider locations, and key information required to decide the actions against the providers reviewed during processing of cases.

All access to UCM NexGen continues to be provided from the CMS Enterprise Portal. The UCM user base will not change through the migration from UCM 1.0. UCM will continue to utilize the existing CMS enterprise authentication method (IDM).

Describe the purpose of the system.

Unified Case Management (UCM) system and associated operational services provide a central repository to support the workload of direct contractors for Centers for Medicare and Medicaid Services (CMS) Program Integrity Contractors (PICs) including Zone Program Integrity Contractors (ZPICs), Program Safeguard Contractors (PSCs), Medicaid Integrity Contractors (MICs), Medicare Drug Integrity Contractors (MEDICs) and future Unified Program Integrity Contractors (UPICs) -- all of which are direct contractors-- across the Medicare and Medicaid programs in their efforts to mitigate fraud, waste and abuse within the programs. This workload includes providing the capability to track leads, audits and investigations; capture and manage workflow activities; report workload metrics; report status of administrative actions and referrals to law enforcement; and record outcomes or disposition of program integrity audit and investigative actions across Medicare and Medicaid programs.

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

The system contains information including the name, work address, e-mail address, work phone number, social security number, Unique Provider Identification Number (UPIN), National Provider Identifier (NPI), medical notes, foreign activities, device identifiers and financial account information of individuals alleged to have violated provision of the Social Security Act or persons alleged to have abused Medicare and/or Medicaid programs. The system will collect PII from CMS employees and direct contractor input (user IDs and passwords). The management and maintenance of the user information to create user accounts for UCM is handled within CMS' Enterprise User Administration (EUA) and CMS Identity Management (IDM).

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

The primary purpose of this system is to collect and maintain information to: (1) Identify a violation or violations of a provision of the Social Security Act or a related penal or civil provision of the United States Code related to Medicare, Medicaid, Health Maintenance Organization (HMO)/Managed Care, and Children's Health Insurance Program have been committed; (2) determine if CMS has made a proper payment as prescribed under applicable sections of the Act; (3) determine whether these programs have been abused; 4) coordinate investigations related to Medicare, Medicaid, HMO/Managed Care and Children's Health Insurance Program (CHIP); (5) prevent duplications of investigatory efforts; and (6) provide case file material to the HHS Office of Inspector General and other federal law enforcement agencies when a case is referred for fraud investigation. UCM will share PII data with CMS legacy systems One Program Integrity (OnePI) and Fraud Prevention System (FPS).

The user ID and password will be collected for internal system users. The management and maintenance of the user information to create user accounts for UCM is handled within CMS' Enterprise User Administration (EUA) and CMS ID Management (IDM).

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
Name
E-Mail Address
Mailing Address
Phone Numbers
Medical Notes
Financial Accounts Info
Device Identifiers
Foreign Activities
Other: Unique Provider Identification Number (UPIN), National Provider Identifier (NPI), User ID and 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

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

The PII is used for CMS fraud, waste and abuse investigations for supporting efforts to protect healthcare expenditures by supporting program integrity functions and combating fraud, waste and abuse in Medicare and Medicaid.
The PII for internal system users is used to gain system access to support system operations.

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

The PII will be used and shared with other CMS legacy systems to validate Fraud, Waste and Abuse (FWA) outcomes, workload and return on investment.

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

Sections 1816(a) and 1842(a) of the Social Security Act provide that public or private entities and agencies may participate in the administration of the Medicare program under agreements or contracts entered with CMS. These Medicare Contractors are known as Fiscal Intermediaries (FIs) and Carriers. FIs have primarily processed bills and made payments for all facilities (hospitals, Skilled Nursing Facilities (SNFs), Ambulatory Surgical Centers (ASCs), etc.). Carriers have primarily processed claims and made payments for all Part B services billed by a physician or supplier.
As part of these contractual duties, FIs and Carriers were charged to perform program integrity activities. These activities include, among other things, reviewing claims to make coverage determinations and auditing provider cost reports. FIs and Carriers performed the entire range of claims processing functions, including entering data, establishing computer edits to identify potential duplicate claims, and mailing notices to beneficiaries and providers. In addition, FIs and Carriers had as part of their responsibilities to deter and detect potential fraud and/or abuse.
Section 4241 of the Small Business Jobs Act of 2010 (Public Law 111-240) mandates the use of predictive modeling and other analytic technologies to identify and prevent fraud, waste, and abuse

in the Medicare Fee-for-Service (FFS) program.

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.

Published: 09-70-0568 (One Program Integrity Data)

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

Hard Copy: Mail/Fax

Within OpDiv

Other Federal Entities

Non-Governmental Sources

Other

Identify the OMB information collection approval number and expiration date

The UCM system does not directly interact with individuals to collect their information. The OMB information collection approval number and expiration date are not applicable.

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.

Memorandum of Understanding (MOU) between Centers for Medicare and Medicaid Services (CMS) & Health and Human Services Office of Inspector General (HHS OIG) and US Department of Justice Federal Bureau of Investigation (DOJ FBI).

Describe the procedures for accounting for disclosures.

The UCM system follows the CMS Acceptable Risk Safeguards (ARS) policy to track all disclosures to third parties. UCM requires that a CMS Data Use Agreement (DUA) is completed and approved by CMS before any disclosure of personally identifiable information is completed. This includes for other federal agencies and contracting partners. The DUA includes the requestor of the data, the record of the data that is being disclosed, and the authority that CMS has for disclosing the information. UCM also ensures that any disclosure to a CMS contracting partner occurs only when a business associate agreement is also in place for this organization to complete work on behalf of the government which would require access to personally identifiable 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.

Information is posted to the UCM system by CMS approved contractors and investigators. Thus, UCM does not directly collect personal information from individuals for the UCM system and does not have a process in place to notify individuals that their personal information will be collected. UCM Systems administrator's user ID and password is collected to authenticate their access to the system. Because this collection is required for them to conduct their required tasks no formal notice is provided to them. The management and maintenance of the user information to create user

accounts for UCM is handled within CMS' Enterprise User Administration (EUA) and Enterprise ID Management (IDM).

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.

The UCM system does not directly interact with individuals to collect their information. As the information posted in the UCM system is used for investigative purposes, there is no option given to individuals to object to the information collection or to opt out.

The collection of this data is required under the Social Security Act for the participation of individuals in the Medicare and Medicaid services. Access to the data can only be obtained through the CMS internal network and requires identification and authorization through CMS EUA and IDM processes. UCM Systems administrator user ID and password is collected to authenticate their access to the system. Because this collection is required for them to conduct their required tasks no opt-out option is available.

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

The UCM system has no process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system. The information in the database is posted by CMS approved contractors and investigators. The UCM system obtains the data from the CMS Shared Services system, CMS One Program Integrity System (OnePI), and the CMS Fraud Prevention System (FPS), therefore these systems as the system of record of the data, they will notify and obtain consent from individuals as major changes occur to the system and the associated data. UCM Systems administrator user ID and password is collected to authenticate their access to the system. Because this collection is required for them to conduct their required tasks, no formal notice is provided to them when there is a major change to the 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.

CMS System of Records Notification Process. Access to the data can only be obtained through the CMS internal network and requires identification and authorization through CMS EUA and EIDM processes.

CMS System of Records Notification Process.

The information is aggregated to support statistical analysis and fraud, waste, and abuse investigations. Information about an individual is processed in support of these investigations.

NOTIFICATION PROCEDURE: For purpose of access, the subject individual should write to the system manager who will require the system name, social security number (SSN) or UPIN, address, date of birth, and sex, and for verification purposes, the subject individual’s name (woman’s maiden name, if applicable). Furnishing the SSN is voluntary, but it may make searching for a record easier and prevent delay.

RECORD ACCESS PROCEDURE: For purpose of access, use the same procedures outlined in Notification Procedures above. Requestors should also reasonably specify the record contents being sought. (These procedures are in accordance with Department regulation 45 CFR 5b.5(a)(2)).

CONTESTING RECORD PROCEDURES: The subject individual should contact the system manager named above and reasonably identify the record and specify the information to be contested. 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).

UCM Systems administrator's user ID and password is collected to authenticate their access to the system. In the event the user's credentials are inaccurate the administrators and system users must contact the UCM service desk to initiate resolution of the issue. The concerns of the administrators and system users will be directly considered, investigated and resolved over the phone or through email exchange on a one-on-one bases by the UCM service desk personnel as required.

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

CMS has safeguards in place for authorized users and monitors such users to ensure against unauthorized use. Personnel having access to the system have been trained in the Privacy Act and information security requirements. Employees who maintain records in this system are instructed not to release data until the intended recipient agrees to implement appropriate management, operational and technical safeguards sufficient to protect the confidentiality, integrity and availability of the information and information systems and to prevent unauthorized access. UCM users take required annual information security and privacy training to receive regular information on this. The UCM system also follows the CMS Acceptable Risk Safeguards which details the requirements for data inspection, integrity, accuracy, and relevancy. If the system should undergo any major significant change to the system, an information security and privacy test is applied to ensure the protection of the PII data contained in the system. Technical controls used include user identification, passwords, security tokens, firewalls, virtual private networks, and intrusion detection systems. Physical controls used include guards, identification badges, key cards, cipher locks, and closed-circuit televisions.

Any PII collected by UCM is in a read-only format. The data will not be able to be modified or destroyed. UCM is the aggregator of the information collected through investigations. It is not the function of the UCM application to validate data contained within the application, any more than it is the function of a word processing application to validate the veracity of the information contained in its documents. Therefore, UCM is not responsible for validating the data and information it aggregates from other sources. Data migration is tested based on source sample data to determine the proper importation of source data.

User IDs and passwords are maintained external to the UCM system in the CMS EUA and IDM systems. UCM roles are administered through a UCM Lightweight Directory Access Protocol (LDAP) server. Access to the UCM LDAP is dependent on valid IDM credentials. If a user role changes, permissions are updated in IDM and these changes are reflected in relevant LDAP provided access. As UCM NeXgen resides in the CMS Amazon Web Services (AWS) cloud environment, all physical infrastructure is managed and maintained by the CMS Cloud Team in concert with AWS. Because UCM is not responsible for the integrity, accuracy or relevancy of non-employee PII it contains there is no mechanism or process to review the data for these attributes.

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.

Account management mechanisms are established for UCM through the CMS Identity Management System (IDM) to identify account types (i.e., individual, group, and system); establish conditions for group membership; and assign associated authorizations. UCM users are granted access based on the assigned duty and intended system use.

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.

Logical access controls and procedures are established for UCM to ensure that only designated individuals can access the CMS information system. UCM team members with CMS IDM and EUA User IDs re-take the CMS online Information Security and Privacy Training course and re-certify the

"System Access" annually via CMS Enterprise User Administration (EUA) Computer Based Training (CBT) Portal to continue accessing the approved CMS system(s). A process has been established for the UCM system when user access is no longer required, due to a change in role on the project or departure from the UCM project team, the UCM Project Manager and the CMS UCM Government Task Leader (GTL) remove the CMS UCM User ID or revoke the specific access privileges that are no longer required.

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 personnel using or administrating the system are either CMS employees or direct contractors. As such all users are required to complete annual CMS Security Awareness Training and Privacy Act Training.

In addition to the Security Awareness training, all UCM contractors are required to complete annual Data Security & Privacy Training and HIPAA Requirements training.

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

The UCM development and DevSecOps team members take annual role-based security training in accordance with National Initiative for Cybersecurity Education (NICE) job roles and CMS recommended 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.

NARA Approved Disposition Authority: DAA-0440-2015-0012

Documents relating to Personal Identifiable Information (PII) and Protected Health Information (PHI) on providers and beneficiaries who have reported that their Medicare information has been compromised and suspects their Medicare information has been stolen through fraudulent methods.

DISPOSITION: Cutoff at the end of the calendar year of the completion of all legal activity. Destroy 7 years after cutoff.

NARA Disposition Authority: NC1-440-79-1/75/23/2B7 FROZEN--DO NOT DESTROY

Files accumulated as a result of allegations or complaints of program abuse or potential fraud by physicians and other providers of services pursuant to sections 206, 208, 1106, and 1107 of the Social Security Act. They consist of complaints from beneficiaries or other sources that are referred to district offices, regional offices, intermediaries, carriers, etc. Included are correspondence, forms, and other papers used in developing and investigating complaints, such as exhibits, copies of claims forms, bills, medical records, investigative reports, fiscal records, and other pertinent physician and provider records.

DISPOSITION: CMS Headquarters and Regional Offices Place in inactive file after final action on the case. Cut off inactive file at the close of the calendar year in which final action was taken, hold 2 additional years, and then transfer to a Federally approved records storage facility. Destroy after a total retention of 5 years.

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

Data is secured according to AWS Security Best Practices and the CMS Acceptable Risk Safeguards (ARS).

Administrative controls include: Documented UCM System Security Plan, Contingency Plan, and Risk Assessment.

Technical Controls include: Multifactor Authentication and Role-Based Access Control to limit access of UCM to authorized users, userIDs and passwords, RSA (product name) Tokens, firewalls, Virtual Private Networks (VPNs), Security Incident and Event Management (SIEM), static and dynamic application security testing, vulnerability management, penetration testing, malicious code

prevention and detection, host intrusion prevention and identification (HIDS), security compliance scanning, infrastructure as code (IAC).
Physical Controls Include (as applicable to TISTA's corporate environments): guards, identification badges, key cards, closed circuit TVs. As UCM NeXgen resides in the CMS AWS cloud environment, TISTA does not manage nor maintain the system's physical infrastructure.