US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/17/2017

OPDIV:

CMS

Name:

Zoned Program Integrity Contractors - AdvanceMed

PIA Unique Identifier:
P-2340102-053752

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.
Agency

Is this a new or existing system?
New

Does the system have Security Authorization (SA)?
Yes

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

Describe the purpose of the system.

The Zone Program Integrity Contractors (ZPICs) and Unified Program Integrity Contract Jurisdiction 1 (UPIC J1) are used to perform fraud and abuse investigations, support benefit integrity efforts, provide medical review support, national and regional data analysis, and law enforcement support. ZPICs and UPIC J1 use a variety of methods to perform its fraud and abuse investigation functions; including reviewing received claims, as well as validating beneficiary, and provider data for Medicare. The overall goal is to reduce improper payments by identifying and addressing coverage and coding billing errors for all provider type.

Describe the type of information the system will collect, maintain (store), or share.
The ZPICs and UPIC J1 collect, maintain and share claims, beneficiary and provider data with the Medicare Fee For Service (FFS) program for the purpose of detecting and preventing fraud, waste, and abuse.

The ZPIC and UPIC J1 process is performed through independent reviews of multiple Medicare Claims and medical records that include PHI and PII information, such as patient’s Health Insurance Claim Number (HICN), beneficiary name, age, date of birth, mailing address, medical records number, patient ICD diagnosis description and notes from the provider about the patient and secondary insurer identification information (if applicable).

The medical claim records also contain public provider information, such as the name of providers and contractors (not direct contractors), their phone number and address.

As part of the Medicare claims reviews, investigators also provide FFS with PII information about the provider that is relevant to the ongoing investigation, such as licensures, certifications, attachments of financial information (bank account numbers, property ownership), and relationships with other entities within their group. The combination of this information is used by investigators to make proper Medicare claim payment determinations.

Approved ZPIC and UPIC J1 users access the system through an Intranet-only application and are prompted to enter in their designated username and password when accessing the system.

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

The purpose of the ZPICs and UPIC J1 programs are to assist CMS with its program integrity responsibilities regarding fraud, waste, and abuse prevention and detection. The contractors who perform this work for CMS are not direct contractors of CMS and shall be referred to as "contractors" throughout the document.

The ZPICs and UPIC J1 collect, maintain and share claims, beneficiary and provider data with the FFS program.

The ZPIC and UPIC J1 use the AdvanceTrack application to track the entire Medicare fraud audit process by recording findings and generating timely and accurate reports based on the claims data that is reviewed.

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

Mailing Address

Phone Numbers

Medical Records Number

Medical Notes

Financial Accounts Info

Certificates

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

Patients

Beneficiaries

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The primary purpose of Personally Identifiable
Information (PII) and Protected Health Information (PHI) for use in ZPICs and UPIC J1 is to ensure correct Medicare claim payment determinations. User credential information is used for authentication to the system in order to access the system as well as for maintenance and operations of the system.

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

There is no secondary use for the PII in the system.

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

The ZPICs and UPIC J1 systems adheres to the Improper Payments Elimination and Recovery Improvement Act (IPERIA, January 2013) as the legal authority governing information use and disclosure.

Sections 205, 1106, 1107, 1815, 1816, 1833, 1842, 1872, 1874, 1876, 1877, and 1902 of the Act (Title 42 United States Code (U.S.C.) sections 405, 1306, 1307, 1395g, 1395h, 1395l, 1395u, 1395ii, 1395kk, 1395mm, 1395nn, and 1396a)

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.

09-70-0568 One Program Integrity Data

09-70-0527 The Fraud Investigation Database

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

State/Local/Tribal

Other Federal Entities

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

Not Applicable. The only direct collection is for user credential information collected by the system for user access logon.

Is the PII shared with other organizations?

Yes

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

Within HHS

PII and PHI is shared with Centers for Medicare and Medicaid Services (CMS), Office of Inspector General (OIG) for Medicare program payment safeguards oversight and ensuring correct Medicare claim payment determinations. Incorrect payments may result in Administrative Actions to include overpayment identification and collection, law enforcement fraud referral, civil and/or criminal monetary penalties.

Other Federal Agencies

PII and PHI may be shared with Department of Justice (DOJ) and Federal Bureau of Investigation (FBI) for law enforcement fraud referral, criminal prosecution, civil and/or criminal monetary penalties.

State or Local Agencies

PII and PHI may be shared with Medicaid Fraud Control Units, Medicaid Program Integrity for program payment safeguards oversight and ensuring correct claim payment determinations. Incorrect payments may result in Administrative Actions to include overpayment identification and collection, law enforcement fraud referral, civil and/or criminal monetary penalties.

Private Sector

The ZPICs and UPIC J1 supports contractor (not direct contractors) user accounts that are required to perform medical record reviews, assist in investigations and data analysis. Contractor administrators are responsible for ensuring the system is operating according to contractual requirements, which includes accessing potential PHI or PII data only on an as-needed basis, such as assisting in investigations. Contract developers are responsible for managing and maintaining the system applications.

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

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

Describe the procedures for accounting for disclosures.

AdvanceMed tracks all request for information through its proprietary application Advancetrack, which keeps a record of the date of the request, what information was released and when and to whom. All AdvanceTrack records are kept offsite at a secure backup facility indefinitely.

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

CMS and Medicare Administrative Contractors (MACs) collect PHI and PII directly from individuals. The role of the ZPICs and UPIC J1 is to conduct audits that identify potential fraud, waste and abuse based on medical records and claim data provided to the ZPICs from CMS and MACs. Therefore providing prior notice to individuals regarding collection of patient PII and PHI related information is not a function of the ZPICs. However, Medicare beneficiaries sign a privacy act notice when they become eligible for Medicare that informs them that information they provide to justify payments will be used to determine the appropriateness of the payment. The PII that is collected for the users, developers and administrators of the system are an assigned. This is required in order to perform their job functions. No prior notice is provided by ZPIC or UPIC J1.

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.

Another CMS system collects PHI and PII directly from individuals, which is then provided to ZPICs and UPIC J1 systems. Therefore, allowing individuals to opt-out is not a function of ZPICs and UPIC J1 systems.

The PII that is collected for the users, developers and administrators of the system are an assigned a unique username and password to log in to the system. This is required in order to perform their job functions. Therefore, there is no option to opt-out provided by ZPIC or UPIC J1.

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

Another CMS system collects PHI and PII directly from individuals, which is then provided to ZPICs and UPIC J1 systems. Therefore, the responsibility of notifying individuals of major changes to the system is not a function of the system.

There is no process to notify users that their PII will change from the original collection. Those that access the system are assigned a unique username and password to log in to the system which do not contain any PII. Therefore, there is no reason for the use or disclosure to ever change.

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.

Another CMS system collects PHI and PII directly from individuals, which is then provided to ZPICs and UPIC J1 systems. Therefore, the responsibility of notifying individuals of major changes to the system is not a function of the ZPICs and UPIC J1 systems.

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

ZPIC and UPIC J1 data analysts are responsible for conducting data quality checks. These checks include loading claims data into test tables, and then performing data quality, analysis and integrity checks on that data. Any issues with the data during these processes are sent to the Baltimore Data Center to resolve either within an internal process review or with the data owner. The Baltimore Data Center analysts then load production tables, run data unduplication and perform unduplication quality checks which follow a similar process as previously explained for claims data.

The ZPICs and UPIC J1 systems infrastructure provides consistent availability through a Multiprotocol Label Switching (MPLS) network, which provides for secure and encrypted communications between all offices, as well as firewall protection against unauthorized intrusions. In addition, backups are performed daily to ensure critical data can always be recovered.

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

Users:

The ZPICs and UPIC J1 support user accounts that are required to perform medical record reviews, assist in investigations and data analysis.

Administrators:

Administrators are responsible for ensuring the system is operating according to contractual requirements, which includes access potential PHI or PII data only on an as-needed basis, such as assisting in investigations.

Developers:

Developers are responsible for managing and maintaining the system applications that are used to perform medical record reviews.

Contractors:

AdvanceMed is contracted by CMS for the purpose of performing user, administrative and developer functions when reviewing medical records and Medicare Claims information.

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

Access to the ZPICs and UPIC J1 systems is based on pre-defined user roles. Therefore, pre-defined user roles govern which permissions system users receive. ZPIC and UPIC J1 users only have access to PII that corresponds with their job function which is approved by a CMS Access Administrator (CAA).

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.

ZPICs and UPIC J1 enforces the concept of least privilege when accessing PII data so that users can access only the minimum amount of PII needed to perform their job function. This is done through first determining the user’s role prior to account creation and then placing users in the appropriate organizational unit that has the predefined least privileges, such as access denied, read-

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.

AdvanceMed provides mandatory CMS Security Awareness and Privacy training to all users on an annual basis which describes the security responsibilities of the users and administrators to protect the confidentiality, integrity and availability of PII and PHI data. Training topics also include the required security mechanisms for storing PII and PHI when not in use, printed on media or sent offsite for archiving purposes.

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

ZPICs and UPIC J1 users and administrators are also trained on the appropriate incident reporting and handling process and procedures in the event of an incident pertaining to PII and PHI.

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 ZPICs and UPIC J1 program information is retained off site at a secure storage facility for a period of 10 years, in accordance with the National Archives and Records Administration (NARA) guideline DAA-GRS-2013-0008-0001

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

All PII and PHI is processed and maintained within a secured environment that complies will all CMS security policies and security requirements. Facilities are secured where PII is stored. This includes physical security components (e.g. hardware, walls, doors and locks).

System security controls also includes those components not directly associated with information processing and /or data/information retention such as scanners, copiers, and printers. PII is protected at rest using an approved method of cryptography consistent with Federal Information Processing Standards (FIPS) 140-2 and National Institute of Standards and Technology (NIST), Special Publication (SP) 800-66 guidance.

Physical media containing PII in transit is controlled using locked cabinets or sealed packing cartons. Privacy controls are built into system design and development processes in order to mitigate privacy risks associated with PII and PHI.

The overall security program provides a comprehensive set of security services to include: privacy and security awareness training, corrective action plans, continuity planning, independent external tests of security controls, risk assessments, system security plans, and incident response planning.