US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/26/2016

OPDIV:

CMS

Name:

Physician Value-Based Modifier

PIA Unique Identifier:

P-1892199-469285

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?

Yes

Identify the operator.

Contractor

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.

In an effort to move from a passive payer to an active purchaser of high-value health care, CMS is developing and implementing a number of value-based purchasing (VBP) initiatives in multiple settings of care. The agency-wide VBP initiatives attempt to correlate the quality of patient care with the cost of the care and includes physician practices, hospitals, nursing homes, home health agencies, and dialysis facilities.

The agency expects VBP to serve as a mechanism for promoting better quality, while avoiding unnecessary costs. This initiative also includes a Physician Feedback Program using Medicare claims and other data to provide confidential feedback reports to physicians that measure the resources involved in furnishing care to Medicare beneficiaries. The Physician Value-Based Modifier (PVM) system supports these initiatives. The Value Modifier provides for differential payment to a physician or group of physicians under the Medicare Physician Fee Schedule based upon the quality of care furnished compared to cost during a performance period.

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

The information collected, maintained or disseminated includes PII such as name, date of birth, social security number, mailing address, phone numbers, medical record numbers, medical notes, military status, financial accounting information, employment, tax ID numbers, employment ID number, name of organization for the purpose of supporting regulatory, reimbursement and policy functions of shared savings programs and to combat fraud, waste and abuse in certain health benefits programs. Submission of this information by providers is required for physicians to receive reimbursement.

The system stores information about its system users- CMS employees and contracting support as well as external users. This includes user ID, email, name, address, and phone number.

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

The Physician Value-Based Modifier (PVM) system uses existing Medicare claims data to implement the value-based purchasing initiatives. Reporting is stored by the system prior to being distributed to providers via the PVM web portal . Reporting contains sufficient claims details to enable the providers to validate the accuracy of the report. In addition, provider reimbursements are calculated and stored by the system.

The system stores information about its system users for authentication, access control, auditing and reporting purposes.

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

E-Mail Address

Mailing Address

Phone Numbers

Medical Records Number

Medical Notes

Financial Accounts Info

Military Status

Employment Status

Taxpayer ID

Other - Organization name, employment ID number, User credentials- user ID, email, name,

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

Employees

Public Citizens

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?

To identify and associate a Provider (Physician Group or Individual Provider) to their registration and their reports, known as the Quality and Resource Use Report (QRUR). QRUR is a report given to providers on quality of care and cost performance. In most cases, PII is Tax Identification Number (TIN) and Name of the Organization. In very few cases, Provider may be using their Social Security Number (SSN) as Billing TIN.

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

In some cases, Tax ID or Employer Identification Number (EIN) for tax purposes.

Describe the function of the SSN.

Tax Identification Numbers (TIN) are being collected for providers in order to calculate their Value Based Payment Modifiers and provide Quality and Resource Use Reports. In very few cases, Provider may be using their Social Security Number (SSN) as Billing TIN.

Cite the legal authority to use the SSN.

Sections 1842, 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)

Standards for Privacy of Individually Identifiable Health Information'' (45 CFR Parts 160 and 164, Subparts A and E) 65 FR 82462 (12–28–00)

Section 1848(p) of the Social Security Act

The Patient Protection and Affordable Care Act Section 3007 (modifying 42 USC 1395w-4).

The Patient Protection and Affordable Care Act Section 2003 (modifying 42 U.S.C. 1396e-1)

Medicare Improvements for Patients and Providers Act of 2008 Section 131 (modifying 42 U.S.C. 1395w–4)

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

Standards for Privacy of Individually Identifiable Health Information.'' (See 45 CFR 164–512(a)(1))

Section 1848(p) of the Social Security Act

The Patient Protection and Affordable Care Act Section 3007 (modifying 42 USC 1395w-4).

The Patient Protection and Affordable Care Act Section 2003 (modifying 42 U.S.C. 1396e-1)

Medicare Improvements for Patients and Providers Act of 2008 Section 131 (modifying 42 U.S.C. 1395w–4)

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

09-70-0503 Fiscal Intermediary Shared System

SORN is In Progress

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

OMB 0938-0734, expiring 12/31/2017

Is the PII shared with other organizations?

Yes

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

Private Sector

The system shares PII directly with physicians who provide health care services for Medicare recipients.

Also, CMS contractors have access to PII to provide support for the system.

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

All participating providers must have a Data Use Agreement (DUA) in place to be able to access the information contained in the Physician
Value-Based Modifier system.

DUAs with physicians describe the information being disclosed and the date and purpose for which it is being shared with them, as well as requirements to which the physicians must adhere.

Describe the procedures for accounting for disclosures.

The reports that are shared with the providers contain the same beneficiary data that the provider submitted to CMS to receive reimbursement. In addition, the reports contain feedback information to correlate the quality of patient (beneficiary) care with the cost of the care. To disclose this data to the physician, a Data Use Agreement must be completed and signed by the provider, and approved by CMS, before accessing the data in the Physician Value-Based Modifier system.

DUAs with physicians describe the information being disclosed and the date and purpose for which it is being shared with them as well as requirements to which the physicians must

adhere.

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 process to notify individuals that their personal information will be collected is performed at the provider level when the beneficiary requests services, which is prior to the information received by the Physician Value-Based Modifier system.

Individuals who participate in the Medicare program are notified in the Medicare & You handbook. The handbook is mailed annually to Medicare beneficiaries.

Provider system users are notified of the collection of their personal information when they complete the Data Use Agreement.

CMS system users are notified in written form when applying for a position.

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.

Beneficiaries who do not want to have their data shared, have the option to decline having their data shared by signing a form or calling 1-800-MEDICARE to opt out of data sharing. Beneficiaries can contact 1-800-Medicare with questions or concerns. There is no loss of benefits to beneficiaries.

Providers are not required to participate in the program, but they must opt-in if they want to participate.

The CMS users 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
09-70-0503 for the Fiscal Intermediary Shared System. For Medicare Part B, the SORN is
09-70-0501 for the Medicare Multi-Carrier Claims System.

For providers with access to the Physician Value-Based Modifier (PVM) system, the providers will be notified when they access the PVM system. Due to the large number of beneficiaries 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 PVM 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.

For providers, the provider contacts the system manager, reasonably identifies the PII data and specifies the information to be contested. The provider states the corrective action sought, and the reasons for the correction with supporting justification. These procedures are in accordance with

HHS department regulation 45 CFR 5b.7.

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

Data accuracy and integrity is maintained through system security and control processes. Control processes include system input edits and recertification of users with access to the system. Periodic privacy audits are performed to ensure the accuracy, integrity and availability of the PII is appropriately maintained. The resulting reports are reviewed by both CMS and providers to verify the accuracy and relevancy of the data.

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

Users:

The providers are the primary users. They review and analyze data and reports.

Contractors:

Review and analyze data and reports.

Others:

Data/production operations teams and Database Administrator's (DBA); required for production support; researchers, data analysts and research team to validate business requirements in the production environment.

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

Access to the system is given based on need to know and job responsibilities to review Medicare claims and reports using a user ID and role based access. Access is obtained by completing a form that must be approved 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 Physician Value-Based Modifier system is given based on need to know and job responsibilities. 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 Physician Value-Based Modifier (PVM) 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 provided by CMS and is modeled on and is consistent with training offered by the Department of Health and Human Services

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 acknowledge 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.

Records are retained in accordance with the NARA schedule III. MEDICARE RECORDS--PROGRAM RELATED, A. Part A

Medicare Claims Records (Disposition Authority: N1-440-04-3.

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 system is given based on need to know and job responsibilities. Physician Value-Based Modifier (PVM) 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:

https://portal.cms.gov

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.

Session Cookies that do not collect PII.

Persistent Cookies that do not collect PII.

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

No

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

No

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

null