US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/13/2017

OPDIV:

CMS

Name:

MicroStrategy

PIA Unique Identifier:
P-5943571-243380

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?
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 significant changes have occurred in the system.

Describe the purpose of the system.
The purpose of Enterprise MicroStrategy BusinessIntelligence (BI) Application is to provide CMS with an Enterprise Solution, which will address these three key business areas: BI Analytical Solutions/Policy Management, Program Management, and Operational Management for all divisions within CMS. MicroStrategy will provide BI reports to aid CMS in detecting fraud and abuse, analyze trends in enrollment, claims and eligibility, and analyze the effectiveness of the Medicare Modernization Act program by allowing the CMS employees and managers access the BI reports, data, and Medicare Modernization Act program indicators.

Describe the type of information the system will collect, maintain (store), or share.
MicroStrategy collects user credentials, user ID and password, from system users for access to the system.

MicroStrategy acts as a pass-through for other CMS systems' data. Data collection and storage is the responsibility of the other CMS systems that utilize MicroStrategy for its reporting function. The type of information that could be used by the other CMS systems to create reports includes: name, address, phone number, date of birth, race, gender, Social Security Number (SSN), Health Insurance Claim Number (HICN), Unique Physician Identification Number (UPIN), medical records and medical records number and medical notes.

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

MicroStrategy is a BI tool that integrates a wide range of reporting, analysis, and information delivery capabilities for other CMS systems to access databases and utilize data to produce reports. For example, some CMS systems use the information passed through MicroStrategy to detect fraud and abuse; analyze trends in enrollment, claims and eligibility; and analyze the effectiveness of the Medicare Modernization Act (MMA) program.

MicroStrategy does not store information but acts only as a pass through from the database store to the CMS system accessing their database store. The information being passed through may contain personally identifiable information of beneficiaries and providers such as contact information, medical records, medical notes, the HICN and UPIN. The systems that are collecting and maintaining this information are responsible for the security parameters and have their own PIAs to address the privacy and security controls in place.

MicroStrategy collects user credentials for user identification access privileges. MicroStrategy system users are CMS employees and direct contractors. Credentials are collected from the user and passed to CMS's Enterprise User Administration (EUA) and Enterprise Identify Management System (EIDM) for verification and validation. User IDs are stored by the system and associated with particular job codes. Job codes determine what information is accessible by the user.

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

Mailing Address

Phone Numbers

Medical Records Number

Medical Notes

Other - HICN, UPIN, User ID and password

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

Employees

Public Citizens

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The primary purpose of PII is for system access and utilization of the MicroStrategy tools.

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

Not applicable.

Describe the function of the SSN.

MicroStrategy does not use the SSN directly. The SSN may be part of the data within a CMS system that uses the reporting feature but MicroStrategy is not directly involved in the collection or function for which that system may use it.

Cite the legal authority to use the SSN.

Sections 226, 226A, 1811, 1818, 1818A,1831,
1833(a)(1)(A), 1836, 1837, 1838, 1843,1866,
1874a, 1875, 1876, 1881, and 1902(a)(6) of the
Social Security Act (the Act).

Section 10332 of the Patient Protection and Affordable Care Act (ACA).

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

Title 42 of the United States Code (U.S.C.):426,426–1, 1395c, 1395i–2, 1395i– 2a,1395j, 1395l(a)(1)(A), 1395o, 1395p,
1395q,1395v, 1395cc, 1395kk–l, 1395ll,
1395mm, 1395rr, 1396a (a)(6), and § 101 of the Medicare Prescription Drug, Improvement and Modernization Act of 2003 (MMA) (Pub. L.108– 173).

Section 10332 of the Patient Protection and Affordable Care Act (ACA); Health Insurance Portability and Accountability Act (HIPAA).

5 USC Section 301 Departmental Regulations

Are records on the system retrieved by one or more PII data elements?

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

Not applicable.

Is the PII shared with other organizations?

No

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

MicroStrategy only collects user credentials. Notification that personal information is being collected occurs at the system log-in, where there is a CMS warning banner advising the user.

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.

To access MicroStrategy, a system user must input their user credentials, PII. Therefore, 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.

If there were any major changes to the system that affected the system users, they would be notified by CMS as part of the normal channels of information. CMS employees or direct contractors give overall consent to the collection of PII and use of government systems as part of the employment or access to systems process.

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.

If a system user has concerns about their PII, they would contact the CMS IT Service Help Desk and report any issues by email or telephone. The Help Desk would investigate and determine if any action needs to be taken by either the user or the IT department to resolve the concerns.

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

MicroStrategy maintains the data integrity and availability by employing security procedures including firewalls, requiring complex passwords, role based access and encryption of user credentials.

The users of the system and MicroStrategy administrators maintain data accuracy and relevancy. Users can correct their own PII data within their own EUA account and administrators run quarterly reports to determine if there are any anomalies (i.e. name change, or mismatch) with user information. If found, the error is addressed and resolved by contacting the user, and modifying their user data, or by removing their access to MicroStrategy if no longer required.

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

Administrators:

System and application administrators may have access to PII for user account management.

Developers:

Developers may access PII in order to perform system updates.

Contractors:

Direct contractors, in their roles as an administrator or developer, may have access to PII as described in those role explanations.

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

Access to PII is managed by the EUA job code assigned to each user. The job codes dictate the permissions to access PII based on the principle of 'least privilege'.

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.

Each CMS system that uses MicroStrategy has separate job codes assigned to the system users. Only users with approved EUA job codes are granted access to the specified MicroStrategy segment and each segment has different access levels, based on role based access control.

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.

CMS employees and direct contractors, who access CMS systems, are required to take the annual Security and Privacy Awareness Training and recertify the training each year. At the end of the training course, a test is taken to verify the completion of the training.

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

Not applicable

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

No

Describe the process and guidelines in place with regard to the retention and destruction of PII.

MicroStrategy follows the CMS Records Schedule published in April 2015, Section IX. Item Which states that records will be destroyed after ten years or when no longer needed by CMS for business needs. The National Archives and Records Administration (NARA) General Records Schedule (GRS) 3.2 031, which states that system access records will be destroyed six years.

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

The administrative controls are: the EUA is leveraged for user authentication and authorization services and conducts annual recertification of user access and privileges; access is disabled when no longer needed; and users are deactivated after 60 days of inactivity. There is also training required for use of the system.

Technical protection is achieved through firewalls and intrusion detection systems; continuous monitoring for system usage and unexpected or malicious activity; the configuration of specialty hardware and the use of encryption, including full disk encryption of laptops and workstations.

The system's physical security controls consist of restricted access and environmental protections. The environmental controls are protected cooling and power sources. Access to this area is recorded, and restricted only to authorized personnel with appropriate security clearance. Facility access is controlled using badge access card readers, security guards present 24/7 and video monitoring.