US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/06/2026

OPDIV:

CMS

Name:

Health Data Reporting

PIA Unique Identifier:

P-7846634-059201

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.

Changes to the Health Data Reporting (HDR) application since the last Privacy Impact Assessment (PIA) include enhancements to support the Center for Medicare and Medicaid Innovation (CMMI) strategic initiative for collecting Health Equity-related data. HDR was updated to enable data transformation to the Fast Healthcare Interoperability Resources (FHIR) standard. Additionally, a connection between HDR and Centralized Data Exchanges (CDX's) Box Service was established. To improve data integrity, the Application Programming Interface (API) for uploading model participant data has been expanded to return status updates from CDX. Future releases will expand the connection to provide Model Teams with an option for transferring the data HDR collects for research and payments.

Describe the purpose of the system.

Health Data Reporting (HDR) is a Center for Medicare and Medicaid Innovation (CMMI) application

whose function it is to collect, validate, store, and disseminate health-related data for CMMI Alternate Payment Models (APM). APM participants submit model specific data via a secured portal where the data is used to monitor the progress towards the intended quality outcomes and cost containment. Payment adjustments are then applied to participant reimbursements based on the expected results.

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

HDR collects, validates, stores, and disseminates APM specific information including health-related CMS beneficiary data, and can include some or all the following data types: electronic health record, administrative, claims, beneficiary/disease registry, survey, clinical trials, vital records and assessments. Types of information include participant information such as the Model ID and Participant Entity ID. HDR also stores beneficiary information including MBI, Name, Address, Phone Number, E-mail Address, Sex, Sex Identify, Date of Birth, Race, Date of Death and Ethnicity. HDR utilizes user ID and passwords, and these login credentials are used to grant access to the system. Users of HDR are the system administrators, maintainers and developers, CMMI staff, model participants and direct contractors. The login credentials (user ID) enabling access to HDR are stored in the CMS Identity Management System (IDM) which has its own PIA.

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

HDR provides APMs functionality to build and store textual and electronic quality measure specifications for quantifying healthcare processes, outcomes, patient perceptions, and other measures that are associated with the ability to provide high-quality health care and/or that relate to one or more quality goals for health care.

APM participants report healthcare related data to HDR via manual entry through a web-based interface, file uploads, or automated means. Data reported can include administrative and medical records, claims data, vital records, surveys, attestations, names, medical notes, date of birth, medical record numbers, and other health related data. Reported healthcare data is stored within an HDR secured database and accessible by APM teams, their respective contractors, and organizations identified in the CMMI Model participant agreement. The reported data is used for calculating quality measures, performing related research, and securing model related data and files (e.g., attestations).

Results of the quality measure calculations are reported to the APMs and participants.

Login credentials enabling access to HDR are provided and stored by IDM which has its own PIA.

Users of HDR are the system administrators, maintainers and developers, CMMI staff, model participants and direct contractors.

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
Date of Death
Medical Beneficiary Identifier (MBI), Sex, Race, and Ethnicity.

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

Business Partner/Contacts (Federal/state/local agencies)
Patients

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

PII is used to uniquely identify the beneficiary for data matching.

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

Data Analysis and Reporting

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

Affordable Care Act (ACA) Sec. 3021

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

No

Master Demonstration, Evaluation and Research Studies for ORDI, SORN 09-70-0591, Pub.

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Other
Government Sources
Within the OpDiv
Non-Governmental Sources
Private Sector

Identify the OMB information collection approval number and expiration date

N/A

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.

HDR does not collect PII information. Individuals' personal information is collected at the point of care by the model participating practitioners. All Medicare participants are provided with a Notice of Privacy Practice that states that although they can elect to not share data for certain processes, as a condition of participating in Medicare, their information will be shared for certain purposes, such as quality assessment and reporting. Alternative Payment Model (APM) Participants are required to inform beneficiaries that they are included in research and provide opt-out procedures. HDR end-users are given Terms and Conditions during the CMS account registration process which include Consent to Monitoring, Protecting Your Privacy, and Consent to Collection of Personal Identifiable Information (PII). Users will be emailed at the email address provided during registration if there are any changes in the Terms and Conditions.

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 provision of PII is "voluntary" as that term is used by the Privacy Act. However, to participate in Medicare programs, participants must provide PII. Individuals' information that is submitted to HDR is collected at the point of care by the model participating practitioners. Responsibility for patient opt-out process resides at the point of information collection from the individual. APM Participants must inform beneficiaries that they are included in research and provide opt out procedures. Alternatively, at any time, beneficiaries may opt out of sharing this data through calling 1-800 MEDICARE or completing a form provided to beneficiaries with their notification. For user credentials, end-users cannot object to providing PII during CMSs authentication system account registration as it is needed to properly verify user identity and create their account. User credentials are provided by CMS's Enterprise User Administration (EUA) system which has its own PIA.

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

The information that is submitted is sourced from existing medical records that have already been collected by the provider. Changes to HDR that would involve changes in uses and disclosures of beneficiaries' PII are not expected to occur. If such changes were to occur, CMS will inform individuals using multiple channels, including direct mailings; notices on the CMS website (including edits to CMS's posted privacy policy), or changes to the relevant systems of records notices. Changes involving uses and disclosures of authentication information are also not expected to occur. In the event of such changes, employees will be notified by notices on the CMS intranet; newsletters; updates to the relevant systems of records notices; e-mails to affected individuals; and through supervisors and system owners.

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.

The information that is submitted is sourced from existing medical records that have already been collected by the provider. Responsibility for patient concerns regarding the use of PII resides at the point of information collection from the individual.

If an individual has concerns that their PII has been inappropriately obtained, used, or disclosed or that the PII is inaccurate, the following procedures should take place:
If the user believes an incident has occurred, the user should cease what they are doing and notify Model Specific Helpdesk. The Help Desk will create a ticket and will notify HDR Management and HDR Security team. HDR security team will investigate the event.

If reportable, security will notify the CMS Help Desk within 1 hour of the incident occurring. (If the event is unreportable, security will notify the Help Desk to close the ticket). The CMS Help Desk Representative will serve as the CMS First Respondent in documenting and assessing the incident to ensure that the incident has been contained. The incident will be escalated and routed to the appropriate CMS group per CMS Incident Response Policy to determine the severity and course of action for mitigation.
System user's credential information is collected via registration with CMS's authentication system, therefore, no process exists for HDR. The issue should be reported to the CMS Help Desk and escalated to the CMS authentication system administrators.

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

HDR does not directly collect data from individuals. The data is sourced from existing records whose business owners are responsible for conducting initial evaluation of Personally Identifiable Information (PII)/Protected Health Information (PHI) holdings and review holdings annually to ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete and reduce PII holdings to the minimum necessary for the proper performance of the documented CMS function for all information systems containing PII/PHI.

Data availability is protected by security controls selected as appropriate. HDR follows the CMS Security and Privacy program and complies with the CMS Acceptable Risk Safeguards, and National Institute of Standards and Technology (NIST) documents such as its Special Publications to select controls appropriate to the level of risk of the system, determined using NIST's Federal Information Processing Standard 199.

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.

User roles are established and managed in a way to ensure that users are only able to access data that pertains to their own organization. Roles are assigned and access is granted, to HDR and the PII it contains, based upon principle of least privilege and "need-to-know" or "need-to-access" requirements to perform their assigned duties.

System Administrators review user accounts at least semi-annually. Any anomalies are addressed and resolved by contacting the user, or by removing their access if no longer required. Activities of all users are logged and reviewed by the system administrator to identify abnormal activities, and if any are found they are reported to the business owner, and the Information System Security Officer (ISSO).

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 enforces role-based access controls, based on a least privilege model, to enforce the protection of data from unauthorized personnel. The application controls data access, such that the organizational user will be restricted to only access the data pertaining to their own organization.

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 CMS employees and direct contractors are required to complete mandatory security and privacy awareness training prior to gaining access to the CMS Network. Each year, thereafter, the user must get recertified. In the event they fail to complete the recertification training, the user's access will be terminated.

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

CMS requires users, on an annual basis, to complete Role Based Training and HHS Records and Retention Training. Employees are also required to complete Annual Refresher Training, and Insider Threat 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 application adheres to data retention and destruction policies/procedures that follow National Archives and Record Administration (NARA) guidelines related to data retention and NIST guidelines related to data destruction. More specifically, HDR adheres to the following NARA general records schedule guidelines: DAA-0440-2015-0007-0001; Destroy no sooner than 10 year(s) after cutoff but longer retention is authorized

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

To secure PII, HDR follows, and the direct contractors are bound by contract to follow, the CMS Security and Privacy program and complies with the CMS Acceptable Risk Safeguards which are aligned to Health and Human Services (HHS) policies and to NIST requirements. HDR PII is secured with security controls as required by the CMS Security Program.

Administrative: Users are provided with privacy training to understand how to properly handle and disclose privacy data. The system uses the principle of least privilege as well as a role-based access control to ensure system administrators, and users are granted access on a "need-to-know" and "need- to- access" commensurate with their assigned duties. Users must receive manager approval to gain access to the system.

Technical: The data in HDR is secured behind a various infrastructure and through application security controls. Technical security controls include, but are not limited to audit controls, user accounts, passwords, and access limitation. All data at rest is encrypted with a Federal Information Processing Standard (FIPS) 140-2 compliant encryption algorithm.

Physical: The Data Center, hosting the application, has security guards and controlled access rooms with locks to guard against unauthorized access.