US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/27/2025

OPDIV:

CMS

Name:

Health Insurance Casework System

PIA Unique Identifier:

P-6101291-011790

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.

Since the last PIA, there have been no significant changes to the HICS system architecture, data handling processes, or user access processes that impacted the system's privacy or security posture. All significant changes undergo a Security Impact Analysis (SIA) to ensure continued compliance with privacy and security requirements. The only change was we updated the Point of Contact (POC).

Describe the purpose of the system.

The Health Insurance Casework System (HICS) is an application that serves as a casework management system for all Affordable Care Act (ACA) Federally Facilitated Marketplace (FFM) health exchange Qualified Health Plans (QHP) and some non-FFM health insurance plans, including self-funded non-federal governmental plans.

HICS provides the tracking and resolution of consumer complaints and issues related to the QHPs (e.g., identity verification, eligibility determinations, denials, appeals, etc.) and to provide reporting data on the program and QHP performance.

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

The information collected by HICS includes the following: consumer name, address, telephone and email address. Other information that may be collected includes demographic (gender, ethnicity, race, date of birth), income, veteran status, health plan information, and employment status. HICS also contains information about the QHP involved in the issue or complaint and includes the QHP name, address, and department name and name of person to contact.

To access the HICS system, HICS caseworkers and system support staff input their user credentials, which contain a user ID and a password.

No additional data types have been included since the last PIA.

Health plan name, Demographics (ethnicity, race, gender), User credentials (User ID and password), Applications IDs, Policy IDs, Subscriber ID.

Social Security Number
Name
E-Mail Address
Phone Numbers
Medical Notes
Military Status
Date of Birth
Mailing Address
Medical Records Number
Financial Account Info
Employment Status
Other: Health plan name, Demographics (ethnicity, race, gender), User credentials (User ID and password), Applications IDs, Policy IDs, Subscriber ID. Provider Transaction Access Number (PTAN), Dependent information, Health Insurance Oversight System (HIOS) ID, and financial information (income).

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

The Physical Security System regularly use PII to retrieve system records including: Applications IDs, Policy IDs, Subscriber ID, Consumer First Name, Consumer Last Name, Consumer Phone Number, Consumer Address, Consumer Email, SSN, Date of Birth, Person Tracking Number (PTN), Dependent information, HIOS ID, Plan Name, Issuer First Name, Issuer Last Name, Issuer Phone Number, Issuer Email, Issuer Address, Any Health-related discussions in the case narrative, and case notes.

Provider Transaction Access Number (PTAN), Dependent information, Health Insurance Oversight System (HIOS) ID, Medical notes, medical record number, and financial information (income).

The HICS casework system manages the complaint process for consumers participating in FFM QHPs and some non-FFM QHPs. On the FFM website, healthcare.gov, there is a link to the Marketplace Appeals Center telephone number and appeals forms. The consumer would then be routed to the HICS system caseworkers. There is no method of creating an appeal online through the healthcare.gov website.

The HICS caseworkers create a consumer case file that contains information about the consumer, the issue causing the complaint, such as an eligibility declination, and the QHP's identity and healthplan in question.

The consumer's information includes their name, address, telephone and email address. Other information that may be collected includes demographic (gender, ethnicity, race), income, veteran status, health plan information, and employment status.

HICS imports some consumer data from the National Data Warehouse (NDW) system; and QHP information from the Multidimensional Insurance Data Analytics System (MIDAS) and the Health Insurance Oversight System (HIOS). Each of those systems maintain their own Privacy Impact Assessment (PIA) for any PII contained in their data.

The system is accessible to a limited community of registered users, including CMS staff and contractors, states' departments of insurance staff, and QHP staff. The users must have a valid CMS issued User ID and password (user credentials) and assigned HICS access permission.

The casework information is maintained for the duration of the case, from initiation until it is resolved. The user credentials are active for as long as the individual is part of the HICS caseworker staff and requires access to the system.

All data that is collected and maintained has been updated above. Current as of 7/14/22.

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
Other: Health plan name, Demographics (ethnicity, race, gender), User credentials (User ID and password), Applications IDs, Policy IDs, Subscriber ID. Provider Transaction Access Number (PTAN), Dependent information, Health Insurance Oversight System (HIOS) ID, and financial information (income).

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

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

PII is used to create a consumer complaint file and contact a consumer to obtain additional information. It is also used for access to the system-by-system users.

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

Not applicable

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

45 CFR 155.200 Affordable Care Act. Title 42 U.S.C.18031, 18041, 18081—18083 and section 1414 and 1411, 26 U.S.C. 6103, and E.O. 9397.

5 USC Section 301 Departmental Regulations

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.

Health Insurance Exchanges (HIX) Program (No. 09-70-0560): Feb. 6, 2013, May 29, 2013 and Oct.

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

Government Sources

Within OpDiv

State/Local/Tribal

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

OMB collection approval not applicable to system user credentials.

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.

HICS has both MOUs and Interface Control Documents (ICD) in place with the other CMS systems, MIDAS, NDW and HIOS for the exchange of information between the systems. The ICDs incorporate both the computer system requirements and the technical requirements that a MOU and ISA would outline.

There are Computer Matching Agreements (CMAs) in place with the state-based health exchanges and the QHP to share information.

Describe the procedures for accounting for disclosures.

There are no disclosures of PII outside of what is permissible for HICS to operate and as outlined in the HIX SORN, updated on October 23, 2013 which specifically references the HICS system. HICS accounts for all disclosures by maintaining records of what information is disclosed to external parties and for what purpose.

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

During the initial case file creation, when created over the telephone, the HICS caseworker will advise that PII will be collected to assist in case resolution. The Appeals form that is completed by the consumer does not specifically notify the individual, but it has to be completed, in order for the appeals process to begin. At system login, the HICS users must accept the HICS Rules of Behavior statement, which includes references to the Privacy Act of 1974, copyright law, and 18 USC 2071, before proceeding into the HICS website. The National Data Warehouse (NDW) system, Multidimensional Insurance Data Analytics System (MIDAS) system, and Health Insurance Oversight System (HIOS) are responsible to provide individual notice and content when major changes occur to their systems. These systems are covered by their own separate PIA's.

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.

There is no option for a consumer to 'opt out' of providing PII as it is essential in creating a case file and resolving their complaint or issue.

For HICS system users, there is not an 'opt out' option, as user credentials are required to access the system and perform their job functions.

The National Data Warehouse (NDW) system, Multidimensional Insurance Data Analytics System (MIDAS) system, and Health Insurance Oversight System (HIOS) are responsible to provide individual notice and content when major changes occur to their systems. These systems are covered by their own separate PIAs.

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

Should any major changes occur the privacy policy on the FFM website, healthcare.gov would be updated. The HIX SORN would also be updated and posted on the Federal Register to inform the public.

The National Data Warehouse (NDW) system, Multidimensional Insurance Data Analytics System (MIDAS) system, and Health Insurance Oversight System (HIOS) are responsible to provide individual notice and content when major changes occur to their systems. These systems are covered by their own separate PIAs.

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 an individual has concerns about their PII, they can contact the Health Insurance Marketplace Call Center at 1-800-318-2596 or the Marketplace Appeals Center at 1-855-1751 and describe their concerns. The call centers would investigate and determine how to resolve the concern.

For HICS system users, they would contact the CMS Information Technology (IT) Help Desk by telephone or email and describe their concern. The Help Desk would investigate and work with the individual to resolve their concern.

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

Complaint records are reviewed and analyzed individually by trained caseworkers as part of the complaint casework and resolution process to ensure the accuracy and relevancy of the information. Additionally, it is also reconciled with the information provided by the HIOS and NDW systems for the integrity and availability. The HICS casework and account functions also utilize data validation edits to ensure data accuracy. This data are encrypted at rest to ensure integrity.

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.

HICS Administrators only grant access to those developers and contractors whose work requires such data, which is based on the principles of least privilege. Administrators review and approve the requests for access to HICS. User accounts are reviewed annually, and any inactive accounts are completely disabled from accessing the system.

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 controls, such as multi-factor authentication for log-on and role-based permissions are the methods that allow the access to PII in the system.

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 HICS users must complete the CMS Information Security and Privacy Group (ISPG) Security Awareness and Privacy training annually. Users acknowledge completion of the training by completing a test and the training system validates the successful completion.

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

In addition to general security awareness training, all HICS users must review the HICS Rules of Behavior, HICS Incident Handling Procedures, and other security considerations specific to their role in developing, maintaining, operating, and supporting HICS. System designers, developers, and administrators also receive training on the technical aspects of addressing specific security issues through peer presentations, mentoring, and the security component of commercial software training materials and courses. Additionally, development contractors are required to send designated staff to the quarterly ISPG security trainings and conferences offered at CMS.

Caseworkers that work with complaint data must attend regular caseworker trainings and meetings as well as abide by standard operating procedures and role-based 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.

Records containing PII will be maintained for a period of up to 10 years after entry into the HICS database. Any records that are needed longer, such as to resolve claims or for audit purposes, will

be retained until those matters indefinitely. Records management adheres to CMS standards and procedures and to National Archives and records Administration (NARA) GRS 5.1 and GRS 5.2., and GRS 4.2, item 130 (DAA-GRS-2013-0007-0012).

Destruction of PII in hard copy and electronic form conforms to procedures and standards for media sanitization specified in CMS Minimum Security Requirements.

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

The security measures in place for HICS to maintain the security of the PII within the system include the following. From an administrative perspective, HICS system users must obtain a CMS User ID and access permissions to log into the system. Periodic review of user accounts and deletion of non-active users. There is role-based access control for users for information the user can access, edit and view. The technical controls include firewalls that prevent unauthorized logon to the system, a tiered system architecture that separates the development/testing environment from the actual system that caseworkers use and encryption of any information that is stored or transferred. The HICS system resides in a CMS Data Center where there are security guards, video monitoring of the facility and facility monitoring systems that ensure the smoke, fire alarm and heating and air conditioning systems are functioning. People entering the facility must present photo identification and verification.