US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

12/22/2016

OPDIV:

CMS

Name:

Health Care Cost Report Information System

PIA Unique Identifier:

P-2752686-222043

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

Due to an HHS policy change the PIA submission has undergone a redesign this year.

Describe in further detail any changes to the system that have occurred since the last PIA.

Not applicable

Describe the purpose of the system.

The Healthcare Cost Report Information System (HCRIS) is the CMS system for aggregating cost report information received from Medicare Healthcare providers via Medicare Administrative Contractors (MAC). The cost report information includes annual statistics, demographics, and financial information about each provider. This information is used by researchers, actuaries and policy analysts in understanding the costs associated with providing healthcare to Medicare beneficiaries.

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

HCRIS collects and stores cost report data which is shared with CMS employees and the public. The cost report data is collected from health care providers who seek reimbursement from CMS for expenses incurred in providing services to Medicare clients. The healthcare provider types include hospitals, skilled nursing facilities, home health agencies, hospices, community health centers, rural health clinics, organ procurement organizations and renal care providers. The data elements include geographic information such as street, city, county, state and zip code; statistics such as the number of beds at a facility, the square footage of space used in providing particular services such as operating room or neonatal care; and financial costs related to operations, training, facility acquisition and management, and management overhead. Other statistics list the number of staff and contractors at a facility, the number of procedures performed categorized by type of procedure, the number of beds maintained for different types of care, and the number of residents or nurses in training in a hospital setting.

HCRIS collects CMS user credentials, specifically the CMS user ID and password, for access control and auditing.

HCRIS uses email addresses provided by the public. This is used to respond to email inquiries about cost report data.

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

HCRIS collects cost report data from multiple Medicare Administrative Contractors(MAC) and provides it to CMS in its databases and to the public in text files. Analysis of the cost report data by these groups is used to gain insight into trends in the provision of healthcare to Medicare beneficiaries. The HCRIS data is used to inform policy makers about the costs of providing healthcare on a national basis and allows researchers to compare different provider's costs and other metrics to identify areas where improvements can be made.

To control access to the HCRIS database and provide audit trails for security purposes, HCRIS requires users to enter their CMS provided User ID and password into their database client tools. HCRIS records the User ID in standard Oracle audit tables on the database server. Access to these audit tables are restricted to HCRIS administrators.

HCRIS receives email inquiries from the public, vendors and contractors about the cost report data and its collection. These emails always contain email addresses and may contain the names, addresses or telephone numbers of the sender. These emails are received by and stored on the Health and Human Services email servers. Emails from vendors and contractors discuss issues with the creation and transmission of the cost reports, while emails from the public are concerned with understanding the content of the reports. Access to these emails is restricted to HCRIS administrators.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Name

E-Mail Address

Mailing Address

Phone Numbers

Other - HHS User ID and password.

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

No

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

The email addresses are used for responding to queries and requests for assistance from employees, contractors, business partners and the public.

The HHS user credentials are used by the security controls in the auditing and access control families.

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.

42 U.S.C. 1395g (section 1815(a) of the Social Security Act).
42 C.F.R. §413.20(b)
5 U.S.C. Section 3 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

Email

Online

Government Sources

Within OpDiv

Other HHS OpDiv

State/Local/Tribal

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

0938-0037, 02/28/2017
0938-1298, 02/28/2019
0938-0107, 09/30/2017
0938-0022, 06/30/2019
0938-0050, 05/30/2019
0938-0758, 02/28/2017
0938-0236, 09/30/2017
09-38-0463, 06/30/2018

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.

All internal users using their User ID receive notification of the CMS policy and procedures concerning privacy on each connection to the network.

External users send emails to HCRIS using a link on the CMS website. The website's privacy page indicates in detail how and when personal information is collected.

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 method for a system user to opt-out of providing PII, their user credentials, because it is required for system access.

For email senders, their email address is required; all other information such as name, address or telephone number is optional. Emails may be sent to HCRIS from resource mailboxes which are not associated with individuals; an example
would be "admin@somecompany.com".

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 and when requesting access to HCRIS data.

If it were necessary to notify an email user of changes to the system, the email address that was collected would be used.

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.

If an email user has concerns about their PII, they would contact the CMS privacy office as published on the CMS website.

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

On a quarterly basis, the CMS Enterprise User Administration (EUA) system (which has its own PIA) provides user IDs and HCRIS related job codes that are compared to user values in the HCRIS system. This is to ensure that least privilege access is enforced with regard to both system access and PII access.

No process is in place to verify the email addresses of senders of emails to HCRIS. The HHS email servers provide SPAM filtering to prevent the accumulation of non-business applicable emails in the mailboxes. The confidentiality and integrity of the emails and their content is provided by role based access to the mailboxes which is reviewed each quarter.

HCRIS has no process in place for reviewing the email data. The integrity of the email store is the responsibility of the enterprise email system.

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

Administrators:

Database administrators require access to auditing records to comply with security controls. The system administrators use the email addresses of inquirers to send responses.

Contractors:

Direct contractors in their role as administrators would have access to PII to support the program objectives.

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

Administrative privileges are require to view the User IDs/email addresses. These privileges are managed by CMS's Enterprise User Administrator 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.

The only PII is the User ID or employees or the email addresses of users accessing the database or sending emails to HCRIS.

HCRIS implements least privilege and role based access to the PII.

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.

HCRIS staff is required to complete the annual privacy and security training provided by CMS.

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

None

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 audit records on the servers are purged automatically by the datacenter after one (1) year. [National Archive and Records Administration, DAA-GRS-2013-0006-0003].

HCRIS Email records are purged automatically after two (2) years. [National Archive and Records Administration N-1-440-6 Item 2].

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

The administrative controls include security training, risk analysis, control development, testing and monitoring. HCRIS personnel are required to complete security and privacy training at regular intervals to ensure current rules and regulations are enforced. Review of auditing records which include login access, record creation and resource consumption is performed daily. HCRIS management and staff have policies and procedures which have been validated by independent assessors to be appropriate for its operation.

Technical controls include providing that all access to HCRIS is controlled by multifactor authentication over encrypted connections. All idle logons are automatically logged off at preset intervals. Password management standards ensure strong passwords which are changed at appropriate intervals. Separation of duties and least privilege principles are applied throughout the system. All users are required to acknowledge their role and responsibility in maintaining the security of the system. Regular updates to the technical and security configuration ensure that the HCRIS data is protected by current software and hardware. This includes VPN, firewall, antivirus and other security technology. Network access administration ensures that all users connecting to the HCRIS system use secured systems.

Physically, the servers that store the PII are housed in secure datacenters with physical and environmental controls that are certified annually. The servers and their software and controls are certified annually to be compliant with the FISMA regulations that apply to them. These datacenters are protected continuously by armed guards and video surveillance to prevent unauthorized physical access and have protections against environmental and natural hazards, including climate control and standby power. Within the datacenters, entry to critical areas is controlled with individual access control cards. The facilities include equipment for the destruction of physical and electronic records.

Note: web address is a hyperlink.