US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/27/2026

OPDIV:

CMS

Name:

CMS FISMA Controls Tracking System-Cloud

PIA Unique Identifier:

P-3000442-504626

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 Changes

Describe the purpose of the system.

The CMS FISMA Controls Tracking System (CFACTS)-Cloud application is a complete centralized system that is located within CMS Amazon Web Services (AWS) and tracks Centers for Medicare and Medicaid Services' (CMS') Federal Information System Management Act (FISMA) systems and their application security deficiencies, Plan of Action & Milestones (POA&Ms), Corrective Action Plans (CAPs), and automates the Certification & Accreditation (C&A) process through the System Development Life Cycle (SDLC). The reporting capabilities allow senior level management to have a clear view of the security posture of all of the applications within CMS. Also, the CFACTS-Cloud application provides a manageable mechanism to provide the Department and Office of Management and Budget (OMB) with required quarterly security posture updates as well as annual assessments for all FISMA applications

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

The CFACTS-Cloud application stores sensitive information pertaining to specific CMS FISMA systems. FISMA security and privacy controls, data diagrams, and security and privacy plans, documents, and agreements are stored and maintained for each system. Personally Identifiable Information (PII) in the traditional sense, Personal Health Information (PHI), or Federal Tax Information (FTI) is not collected, maintained, or stored within CFACTS-Cloud. Only privileged users have access to the CFACTS-Cloud application. Information collected on users is point of contact (POC) information including full name, desk and work cell phone numbers, email address, desk and office location.

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

The CFACTS-Cloud application stores sensitive information pertaining to specific systems. System security and privacy controls, data diagrams, security and privacy plans, agreements and documents are only visible to personnel within CMS' Enterprise User Administration (EUA) user authorized roles. EUA is covered by its own separate Privacy Impact Assessment (PIA). This documentation and information tracks Centers for Medicare and Medicaid Services' (CMS') Federal Information System Management Act (FISMA) systems and their application security deficiencies, Plan of Action & Milestones (POA&Ms), Corrective Action Plans (CAPs), and automates the Certification & Accreditation (C&A) process through the System Development Life Cycle (SDLC). This allows senior management to have a clear view of the security posture and also provides OMB with required quarterly and annual security posture updates.

Information collected on users is point of contact (POC) information including full name, desk and work cell phone numbers, email address, desk and office location. It is used in order to provide CMS system stakeholder contact information as well as user account creation.

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: Desk and office location.

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

Employees
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

5,000-9,999

For what primary purpose is the PII used?

The PII is used in the contact application as part of the Business Continuity plan solution. This is to keep track of the individuals to contact for Contingency Planning (CP)/Disaster Recovery (DR) activities. The basic user information such as name, desk phone and/or work cell phone numbers, desk or office location, and email address is received during the creation of account in CFACTS-Cloud.

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

There is no secondary use of the PII.

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

5 USC 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

Email

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Other

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.

No prior notice is given by CFACTS-Cloud, as the system user PII is collected by CMS' EUA which has its own separate PIA.

EUA has dedicated policies and processes for notifying and providing consent to individuals about collecting their data.

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 PII that is collected is in a separate application, which is the EUA, therefore there is no ability to opt-out. EUA has dedicated policies and processes for notifying and providing consent to individuals about collecting their data. EUA is covered by its own PIA.

If the user requires access to CFACTS-Cloud, they cannot 'opt-out' of providing their PII to EUA, as the user ID, name, phone number, email address, and desk/office location are the identifiers used to create the user within the application's security module.

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

No notification process is given by CFACTS-Cloud, as the system user PII is collected by CMS' EUA which has its own separate PIA. EUA has dedicated policies and processes for notifying and providing consent to individuals about collecting their data.

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.

There is no process in place to resolve an individual's concerns by the CFACTS-Cloud system as

the PII within CFACTS-Cloud is provided by EUA.

Individual's concerns involving their PII (user credentials), are addressed by the Enterprise Administration User team (a function of the maintenance contractor, Leidos). The CMS IT service desk personnel will assist in rectifying any incorrect user identification information within EUA.

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

In order to maintain the integrity, availability, accuracy, and relevancy of the PII stored within the database, the System Administrator, semiannually, performs a crosswalk between the EUA listing of individuals with the job code CFACTS_USER_P and CFACTS-Cloud's listing of active users. Any anomalies (i.e. name change, or mismatch) are addressed and resolved by contacting the user, and modifying their user data, or by removing their access to CFACTS-Cloud, if no longer required under their current job description.

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.

Only the System Administrator and the Developer have access to PII. All other users do not have access to PII stored in CFACTS-Cloud. User Privileges (role based) are defined within the Security Module. The initial EUA request for approval for access to the CFACTS-Cloud application describes the level of access (need to know) required by the individual.

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.

User Privileges (role based) are defined within the Security Module. The initial EUA request for approval for access to the CFACTS-Cloud application, describes the level of access (need to know) required by the individual.

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 CFACTS-Cloud users must annually complete CMS User ID Certification (which involves a review of all applications to which they have access) through the CMS Information Systems Security and Privacy Awareness Training and Cyber Awareness Training, and Records Management Training.

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

The team conducts periodic security training throughout the year on a variety of relevant topics. In addition, twice annually, CMS business owners receive targeted security and privacy training through the CMS Security Control Oversight and Update Training (CSCOUT) program, which covers timely and applicable security and privacy subject areas.

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.

National Archives Records Association (NARA), General Records Schedule (GRS 5.1 and 5.2 states that CFACTS will destroy/delete when 7 years 6 months, 10 years 6 months, or 20 years 6 months old, based on the maximum level of operation of the Certification Authority, or when no longer

needed for business, whichever is later.; and GRS 24 states that CFACTS will delete/destroy when agency determines they are no longer needed for administrative, legal, audit or other operational purposes. The EUA system that provides the database with PII to CFACTS destroys the data. When the nightly updates sync with the CFACTS, then the data that is no longer needed is removed from EUA and does not appear in CFACTS.

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

Physical controls such as the security of the physical server, which include such items as providing long term power supply, emergency lighting, and fire protection; Physical controls are in place such as security guards to ensure access to the buildings are granted to only authorize individuals. Identification of personnel is checked at the facility. CFACTS is built using industry best practices and independently reviewed against Federal Information Security Management Act (FISMA) and National Institute of Science and Technology (NIST) Security and Privacy controls to ensure technical, operational, and management controls are properly applied Technical controls are in place such as the Data Center manages remote access, equipment ordering/testing, and has responsibility for the EUA system (management of user accounts), which defines the privileges for each user of the information system(s); Office of the Chief Information Security Officer (OCISO) coordinates compliance with security controls and the artifacts that document compliance by each application; and General Support System (GSS) manages, among others, telecommunications, remote access, and transmission confidentiality. As the physical and technological aspects are managed by other organizations within CMS, and as access to CFACTS is a function of Host on Demand (HOD) and EUA, the duties of the System Administrator are solely, that of administration. Administrative controls are at the application level, although CFACTS-Cloud has built-in internal controls to enforce role-based access to datasets and functions, it is the responsibility of the System Administrator to enforce the Segregation of Duties Policy to ensure that each role has limited responsibility (user roles are defined to only allow access to specific functions of the application. PII is secured on the system level, through compliance with the policies in place, developed to accomplish that task. This involves the annual submission, by the System Administrator, of a System Security Plan (SSP), Information Security Risk Assessment (IR RA), Contingency Plan (CP), completion of the Privacy Impact Assessment (PIA), and adherence to the Security Controls.