US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/21/2026

OPDIV:

ACF

Name:

Credal Artificial intelligence Corporation (Credal AI)

PIA Unique Identifier:

P-6031084-775127

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.

Internal Flow or Collection

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

Since the last PIA submission, several updates have been made to reflect current system functionality and documentation. These updates include: (1) revising the terminology from “copilots” to “agents” to align with the product feature rename; (2) adding additional detail regarding data integrations, including the potential for bidirectional data exchange when users configure Actions that Credal Agents can take on their behalf to update information in external systems; (3) removing references to the deprecation of the auto-redaction feature in Credal, which is being sunset in favor of enterprise-grade large language model subscriptions from Microsoft Azure and Amazon Web Services; (4) removing the statement that audit logs are retained “permanently,” reflecting the implementation of shorter log retention policies; (5) adding State/Local/Tribal entities and the Private Sector as potential sources of PII; (6) clarifying that the term “direct employees” includes both federal and contractor personnel; (7) updating the description of security training for Credal administrators to reflect that all administrators complete privileged Rules of Behavior training, and that some, but not

all, hold security certifications; (8) adding biometrics and resumes as types of PII that may be used due to integration with ACF enterprise Box system

Describe the purpose of the system.

Credal Artificial intelligence (AI) is a software platform that allows employees at Administration for Children and Families (ACF) to build AI-powered tools, called workflow assistants, to simplify and improve their daily tasks. For example, these assistants, called "Agents," can summarize meeting notes or aid in filling out security controls for the ATO (Authority to Operate) process. Employees access Credal through a web application, where they can interact with advanced AI tools, known as large language models (LLMs). These models are designed to understand and generate human-like text, enabling users to chat with AI or create customized assistants for specific tasks.

Credal connects securely to Administration for Children and Families (ACFs) internal tools, like SharePoint and Box, so that employees can use AI with ACF data. The platform includes privacy and security features, such as creating logs of all user activity, which administrators can monitor to ensure personal identifiable information (PII) is handled securely.

For developers, Credal provides an interface (called an API - an application programming interface) to build additional tools on top of the platform, leveraging its AI features and security capabilities.

Credal helps ACF employees work more efficiently while ensuring data privacy and security are maintained.

Credal AI Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks.

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

Credal ensures privacy and data protection for all users and information handled through the web application by collecting only the data explicitly chosen by users and implementing advanced security measures. Credal collects and uses the following types of information:

1. User Login Information:
Credal connects to ACF’s secure login system, Okta (Single Sign-On), to authenticate users. This process collects each user’s name, email address, profile photo, and group assignments. Group assignments are used to determine the user’s permissions and access levels within Credal. This login information is required for all employees who use the Credal platform.

2. Productivity System Data:
Credal integrates with ACF’s internal productivity tools, including Box, SharePoint, and Confluence. Users can choose which specific documents or data to use within Credal based on their tasks. Only the data explicitly selected by users is collected and stored in Credal.

Depending on the selected documents, this data might include Personally Identifiable Information (PII) such as names, email addresses, phone numbers, dates of birth, mailing addresses, legal documents, Social Security Number (SSNs), Driver License Numbers, Mother maiden names, medical notes, certificates, education records, military status, foreign activities, biometric identifiers, vehicle identifiers, medical record number, financial account information, device ID, employment status, passport number, Employer Identification Number (EIN), demographics, resumes, and taxpayer identification numbers (TINs) for companies. The purpose of Credal in handling these types of PII depends on the task or workflow being supported, such as reviewing legal contracts or managing correspondence.

3. Data Storage and Security:
All data collected in Credal is securely stored within ACF's government-owned cloud environment, ensuring it remains in a controlled and protected setting. ACF integrates its own large language models (LLMs) into Credal through enterprise-grade subscriptions, including Microsoft Foundry and Amazon Web Services Bedrock. This approach ensures that ACF data is not used to train underlying models and remains the property of ACF

Data ingested into the system is not shared with external model providers beyond what is necessary for processing. Enterprise-grade LLM services are used through Microsoft Azure OpenAI (via Foundry) and AWS Bedrock, and data is not used to train the underlying models.

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

Credal is a secure platform that allows employees at ACF to create and use workflow assistants, also called Agents, to help with tasks such as summarizing meeting notes or managing grants. The system collects, maintains, and shares the following types of information:

1. User Login Information:
Credal uses ACF's Okta Single Sign-On (SSO) system to authenticate users when they log in. This process collects the user's name, email address, profile photo, and group assignments.

The user's email address is used to uniquely identify their account in Credal.

The user's name and profile photo are displayed in their profile and used for collaboration within the platform.

Group assignments determine what actions users can perform using role-based access controls (RBAC). For example, an administrator may have broader permissions than a general user.

2. Productivity System Data:
Credal integrates with internal ACF systems including SharePoint, Box, Confluence, Jira, GitHub, and GitLab. Users select specific documents or data from these systems to build their workflow assistants. Credal only surfaces content from document users have access to in the source systems. In some integrations, the user specifically restricts which files are shared with Credal. In other integrations, Credal has the ability to search the contents of all files the user has access to in the source system and pull in the most relevant context to the user's query. Some integrations are also bidirectional, where the user can configure specific Actions that Credal can take on their behalf to update information in the integrated system.

Examples:

Meeting Notes Summarization Agent:
A user may build an Agent to summarize meeting notes. This might require access to meeting notes stored in SharePoint and a Confluence page with best practices for summaries. The meeting notes might include PII such as the names of meeting participants.

Grant Management Assistant:
A user may build an Agent to assist in grant management. This may involve accessing grant applications stored in Box and related agreements. Grant applications could include PII such as names, email addresses, phone numbers, and taxpayer IDs for companies.
Additionally, depending on the task or workflow being supported, the system may also process Social Security numbers (SSNs), driver's license numbers, mother's maiden names, medical notes,

certificates, education records, military status, foreign activities, biometric identifiers, vehicle identifiers, medical record numbers, financial account information, device identifiers, employment status, passport numbers, Employer Identification Numbers (EINs), demographic information, and resumes

3. Data Management and Retention:
All data collected by Credal is stored securely in ACF's government-owned cloud. Administrators can view all stored data in the system's Data Catalog, where they can delete any data that is no longer relevant.

Credal enforces the same access permissions as the original source systems. For example, if a document in SharePoint is only accessible by two people, Credal ensures it remains accessible only to those same individuals.

Users and administrators can delete files in the Data Catalog when no longer needed. However, user prompts (the questions or commands users provide to workflow assistants) are stored for a set period of time for auditing purposes to ensure compliance and system accountability. These prompts are secured and access to them is restricted to authorized personnel.

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
Photographic Identifiers
Driver's License Number
Biometric Identifiers
Mother's Maiden Name
Vehicle Identifiers
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Financial Accounts Info
Certificates
Legal Documents
Education Records
Device Identifiers
Military Status
Employment Status
Foreign Activities
Passport Number
Taxpayer ID
Company Taxpaer IDs, e.g. Employer Identification Number (EIN)
Demographic Information
Resumes

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
Benefit program participants

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

There are two primary purposes for using PII in Credal:

1. User Authentication and Profile Creation:
Credal collects user credentials to securely authenticate HHS employees when they log into the platform. The system uses the user's email address as a unique identifier for their account. Additionally, the user's name and profile picture are used to create their profile in the application and enable collaboration with other users.
Group assignments are used to determine what actions each user can perform within the platform, based on role-based access controls (RBAC). For example, administrators may have access to manage system settings, while general users can only create workflow assistants or access specific data.

2. Workflow Assistant Enablement:
Documents connected to Credal to support workflow assistants may sometimes include PII about employees, vendors, or public citizens. For example, a workflow assistant designed to assist with grant management might access grant applications or related documents that include PII such as names, email addresses, phone numbers, and taxpayer identification numbers (TINs).

These documents are selected explicitly by users for their workflows, and Credal ensures that PII in these documents is handled according to the permissions set by the source systems.

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

Not applicable. There are no secondary uses of PII in the system aside from the primary uses.

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

5 USC 301, Departmental Regulation.

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
Other
Government Sources
Within the OPDIV
Other HHS OPDIV
State/Local/Tribal
Other Federal Entities
Non-Governmental Sources
Public

Identify the OMB information collection approval number and expiration date

Not Applicable

Media/Internet
Private Sector

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.

1. User Login Information:

When a user logs into Credal using Okta Single Sign On (SSO), they are shown a consent screen. This screen clearly explains what personal information (such as their name, email address, and profile picture) will be shared with Credal. Users must provide their consent by accepting or denying the request before proceeding. This consent screen is displayed each time a user logs into Credal to ensure they are aware of the data being shared.

2. PII in Productivity Systems:

If a user connects documents containing PII from productivity systems like SharePoint or Box to Credal, notification about this data collection is the responsibility of the originating system. For example, SharePoint or Box provides notice to users when PII is added or stored in those systems.

3. Limitations on Notice:

In some cases, the PII accessed by workflow assistants may include information about other individuals, such as meeting participants or grant applicants. Credal does not provide direct notification to these individuals, as the responsibility lies with the original system where the PII was 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.

Credal ensures that users' preferences are respected while maintaining secure and compliant operations by relying on the source systems for opt-out functionality and ensuring synchronization.

Individuals can opt out of the collection or use of their PII through the systems that originally collect their information. Credal does not collect PII directly but relies on data from the following systems:

1. User Login Information:
For user login data collected through Okta Single Sign-On (SSO), individuals can contact the Okta system administrator or follow Okta's opt-out process to request the removal of their information.

2. Productivity System Data:

For PII included in documents connected to Credal (e.g., SharePoint, Box, or Confluence), individuals must use the opt-out mechanisms provided by those systems. These systems are responsible for notifying users about their opt-out options.

3. How Credal Handles Opt-Out Requests:
Credal automatically syncs data with Okta SSO and connected productivity systems every 24 hours. This means that if a user opts out of sharing their PII with a source system and their PII is deleted or restricted in that system, Credal will update its records accordingly within one day.

4. Limitations and Safeguards:
Credal does not provide a direct opt-out option for PII contained in documents selected by users, such as meeting notes or grant applications. In these cases, the responsibility to notify and handle opt-out requests lies with the original systems where the data was collected.

5. Credal Minimizes Risks:

a. Credal enforces access permissions defined by the source systems to ensure that PII is only visible to authorized users.

b. Users have control over which documents they choose to connect to Credal and can remove documents from the platform if they no longer wish to use them in workflow assistants.

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

1. PII from Source Systems:

Credal does not collect PII directly. Instead, it relies on systems such as Okta SSO for user login information and productivity platforms like SharePoint or Box for document-based PII. These systems are responsible for notifying individuals if the use of their PII materially changes, as they are the original collectors of the data.

2. Consent at Login:

When users log into Credal through Okta SSO, they are shown a consent screen. This screen explains what user information (e.g., name, email address, and profile picture) will be shared with Credal. Users must either provide or deny consent before accessing Credal.

3. Major Changes in Credal:

If Credal makes significant changes to how it uses or shares PII, it will provide notifications to affected users through in-platform alerts or email communications. This includes changes to data-sharing practices, new system integrations, or updates to privacy policies. For example, if Credal begins using PII for new types of analysis or sharing data with third-party partners, users will be notified in advance and given the option to provide or withdraw consent.

4. PII in Documents Shared by Users:

For PII contained in documents selected by users (e.g., meeting notes or grant applications), notification is not provided directly to the individuals mentioned in those documents. This is because Credal relies on the source systems, like SharePoint or Box, to manage notifications for individuals whose data is included in stored documents.

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.

Credal does not collect personal information directly from the public. Instead, it uses PII from external systems, such as Okta SSO for user login information or productivity platforms like

SharePoint and Box for document-based PII.

If an individual believes their PII has been inappropriately obtained, used, or disclosed through Credal, or if they believe the PII is inaccurate, the following process is in place to address their concerns:

1. Submitting a Concern:
Individuals can report concerns about PII handling to their organization's system administrator or privacy office. This includes concerns about data originating from connected systems, such as inaccurate information in SharePoint documents or unauthorized access to user profiles.

2. Investigation and Resolution:

a. Credal administrators will coordinate with the source systems (e.g., Okta SSO, SharePoint) to investigate the issue. This may involve verifying access logs, reviewing audit trails, and confirming permissions to determine whether the PII was obtained, used, or disclosed inappropriately.

b. If the PII is found to be inaccurate, Credal will synchronize updates with the source system after the correction is made there.

3. Escalation:
If the issue cannot be resolved through the standard process, it will be escalated to the organization's privacy office or designated data protection officer for further investigation and resolution.

Limitations:

Because Credal relies on external systems for PII, it does not have direct control over correcting inaccuracies or providing notice to individuals outside the system. However, Credal enforces access controls and permissions inherited from source systems to minimize the risk of PII misuse or unauthorized disclosure.

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

Credal ensures that the PII it manages remains secure, accurate, and relevant to its intended purposes by combining automated tools, synchronization with source systems, and periodic manual reviews.

Credal has several processes and tools in place to periodically review and maintain the integrity, availability, accuracy, and relevancy of PII:

1. Integrity
Credal performs regular, automated backups of its database to protect PII from system failures or data corruption. These backups are tested periodically to ensure they can be successfully restored if needed. System integrity is also supported by built-in monitoring tools that alert administrators to potential data corruption or inconsistencies.

2. Availability
Credal uses high-availability (HA) services to ensure that PII remains accessible, even during temporary service disruptions. These services are continuously monitored to detect and resolve any performance issues.

3. Accuracy
PII accuracy is maintained by synchronizing data with the source systems daily (e.g., Okta SSO, SharePoint, or Box). Any updates or corrections made in the source systems are automatically reflected in Credal, ensuring that the data remains accurate as long as it is correct in the original systems.

4. Relevancy
Credal's Data Catalog allows system administrators to monitor all PII connected to the system and assess its usage. Administrators can create and enforce policies to remove outdated or irrelevant data, such as data that has not been accessed or used by workflow assistants within a specific period. Administrators review the Data Catalog at least once per quarter to identify and remove such data.

5. Periodic Reviews and Monitoring
a. System administrators perform quarterly reviews of the Data Catalog to ensure data integrity, identify unusual activity, and confirm compliance with privacy policies.
b. Platform Action Audit Logs are reviewed regularly to detect unauthorized access attempts or suspicious activity involving PII. Any issues identified are investigated promptly, and corrective actions are taken as needed.

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.

Credal ensures that only authorized individuals can access PII in accordance with their roles and responsibilities by combining synchronized source system permissions, role-based access controls, and strict oversight.

1. Source System Permissions:

Credal synchronizes data from ACF productivity systems (e.g., SharePoint, Box) and enforces the same access permissions as those systems. Users can only access data in Credal if they are authorized to access the same data in the source system. This synchronization occurs automatically, so any changes to permissions in the source systems are immediately reflected in Credal. This ensures that no one gains access to PII they are not already permitted to access.

2. Administrator Access:

Administrators are granted access to PII based on their responsibilities for governance, oversight, and system maintenance. Access is determined by role-based access controls (RBAC) and requires approval from the organization's system administrators or privacy officials.

3. Developer Access:

Developers may access PII in application logs only when necessary to resolve technical issues.

Access to these logs is limited to specific debugging scenarios and is reviewed on a case-by-case basis to ensure PII exposure is minimized.

4. Contractor Access:

Some contractors are users of the system, in which case their access to PII is as stated for the broader User category. Other contractors who are not users of Credal are not granted access to PII unless explicitly authorized for a specific business need such as troubleshooting a login issue. In such cases, access is restricted to the minimum amount of PII necessary to perform their duties, and contractors must comply with organizational privacy policies and agreements.

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.

Credal ensures that users only access the minimum amount of PII necessary to perform their jobs by combining user-controlled data connections, strict enforcement of source system permissions, task-specific filtering, and role-based access controls.

User-Controlled Data Connections:
Users control what data they connect to Credal, ensuring that only data relevant to a specific workflow assistant or task is brought into the system. For example, if a user needs to summarize meeting notes stored in SharePoint, they can connect only the specific document required for that task.

Source System Permissions:
Credal respects the permissions set in the source systems (e.g., SharePoint, Box, Confluence, Jira, GitLab, and any other future integrations). Users can only access data they are already authorized to view in the source system. For example, if Bob connects a document from SharePoint that is restricted to himself and Alice, Credal ensures that no other users can access the document.

Task-Specific Data Filtering:
Credal uses intelligent filtering techniques to ensure that PII is surfaced only when it is directly relevant to a user's question or workflow. For instance, if a user requests assistance with summarizing a document, Credal will only surface the data required to generate the summary, leaving irrelevant PII hidden.

Role-Based Access Controls (RBAC):
Access to features and data within Credal is further limited based on user roles. For example, administrators may have broader access for governance purposes, but developers only access logs containing PII when necessary for debugging.

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.

Credal ensures that all personnel are equipped to protect the information they access and maintain by addressing the specific needs of each role and emphasizing accountability.

1. Credal Staff:

a. All Credal administrators receive advanced security training including the HHS Privileged User Rules of Behavior.

b. Training includes insider threat awareness, strict access control practices, and segregation of

duties to minimize the risk of unauthorized access or misuse of data.

c. Regular refresher courses and updates are provided as organizational policies and Credal functionality evolve.

2. ACF Users (Employees and Contractors):

a. ACF users receive training on the responsible use of GenAI tools, including: (i) the purpose and limitations of GenAI use, (ii) identifying and mitigating risks associated with GenAI use, and (iii) understanding the types of data prohibited from being ingested into Credal.

b. Training is provided before users set up their accounts to minimize improper or risky use of Credal.

c. Ongoing learning support is offered to keep users informed of new functionalities and evolving policies. For example, we hold weekly office hours and send regular updates to users about new features and developments.

d. Offline training materials, such as recorded sessions and PowerPoint presentations, are available to all users for flexible access.

e. All ACF staff are required to complete general security and privacy awareness trainings.

Training content is reviewed and updated regularly to reflect changes in Credal functionality, privacy policies, and emerging security risks.

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?

Yes

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

Data retention in Credal is fully configurable, meaning the government has full control over how long data is retained, and what other retention rules are put in place. Credal works with the government to set up automated retention as necessary.

Data is retained per General Record Schedule (GRS) 5.2 Item 020 Temporary. Destroy upon creation or update of the final record, or when no longer needed for business use, whichever is later. (DAA-GRS-2022-0009-0002)

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

1. Administrative Controls:

Administrators within ACF will have the ability to control who has access to the Credal platform by assigning user access within Okta SSO. They use Okta SSO to ensure that the system is only accessible to those within ACF and restrict access to anyone outside of ACF.

2. Technical Controls:

Login to the system is implemented via a connection to Okta SSO, using the OAuth2 protocol, which is an industry standard. Okta implements MFA (multi-factor authentication), which ensures that only authorized users can gain access to Credal, even if a single factor of their authentication is breached (e.g., their password is leaked). Okta also allows administrators to assign specific users or groups to have Credal access, so only users who need access will get it.

Data stored within Credal is secured on the backend through a set of industry standard zero-trust security practices, including data encryption in transit and at rest. Further details on the application security of Credal may be found in the Credal trust center at https://trust.credal.ai/.

Credal is deployed within ACF's NGSC (Next Generation Secure Cloud), which allows the application to inherit several infrastructure security controls in place within NGSC.

3. Physical Controls:

Credal is hosted inside NGSC, which is within AWS (Amazon Web Services), so the physical controls in place are provided by AWS. These controls include fire detection and suppression requirement, uninterruptible power supply (UPS) units, climate control, preventative maintenance, video surveillance and security staff, and a thorough access control policy.