US Department of Health and Human Services

Third Party Websites and Applications Privacy Impact Assessment

Date Signed:

October 10, 2019

OPDIV:

CMS

Name:

DocuSign – For the Eligibility Appeals Case Management System

TPWA Unique Identifier:

T-6865336-440788

Is this a new TPWA?

Yes

Will the use of a third-party Website or application create a new or modify an existing HHS/OPDIV System of Records Notice (SORN) under the Privacy Act?

No

If SORN is not yet published, identify plans to put one in place.

Not Applicable

Will the use of a third-party Website or application create an information collection subject to OMB clearance under the Paperwork Reduction Act (PRA)?

No

Indicate the OMB approval number expiration date (or describe the plans to obtain OMB clearance).

Expiration Date: 1/1/01 12:00 AM

Describe the plans to obtain OMB clearance.

Explanation: Not Applicable

Does the third-party Website or application contain Federal Records?

No

Describe the specific purpose for the OPDIV use of the third-party Website or application:

As a result of the 2010 Affordable Care Act, the Department of Health and Human Services (DHHS) was tasked to implement the Federally Facilitated Exchanges; as a result of the Federal Health Exchange system being implemented, the Eligibility Appeals Case Management Systems (EACMS) was established to support the Eligibility Appeals Operations Support (EAOS) contract.

The Eligibility Appeals Operations Support created the process of allowing potential appellants the ability to submit appeals online through the Healthcare.gov website and DocuSign Connect Electronic Signature services. Online Submission will allow healthcare appeals to be processed at an expedient pace as it removes the need for Appellants to mail or fax in paper forms. It also allows for quicker data entry for appellant information into EACMS.

Have the third-party privacy policies been reviewed to evaluate any risks and to determine whether the Website or application is appropriate for OPDIV use?

Yes

Describe alternative means by which the public can obtain comparable information or services if they choose not to use the third-party Website or application:

Paper appeals can still be mailed to CMS for processing.

Does the third-party Website or application have appropriate branding to distinguish the OPDIV activities from those of nongovernmental actors?

Yes

How does the public navigate to the third party Website or application from the OPIDIV?

An external hyperlink from an HHS Website or Website operated on behalf of HHS

Please describe how the public navigate to the thirdparty website or application:

The public can navigate to DocuSign through their browsers by accessing the links from https://www.healthcare.gov/

If the public navigate to the third-party website or application via an external hyperlink, is there an alert to notify the public that they are being directed to anongovernmental Website?

Yes

Has the OPDIV Privacy Policy been updated to describe the use of a third-party Website or application?

Yes

Provide a hyperlink to the OPDIV Privacy Policy:

https://www.healthcare.gov/privacy/

Is an OPDIV Privacy Notice posted on the third-part website or application?

Yes

Is PII collected by the OPDIV from the third-party Website or application?

Yes

Will the third-party Website or application make PII available to the OPDIV?

Yes

Describe the PII that will be collected by the OPDIV from the third-party Website or application and/or the PII which the public could make available to the OPDIV through the use of the third-party Website or application and the intended or expected use of the PII:

Social Security Number
Date of Birth
Name
Photographic Identifiers
Driver's License Number
E-Mail Address
Mailing Address
Phone Numbers
Medical Notes
Financial Accounts Info
Legal Documents
Employment Status
Passport Number
Taxpayer ID
Citizenship Immigration Status,
Veteran Status

Describe the type of PII from the third-party Website or application that will be shared, with whom the PII will be shared, and the purpose of the information sharing:

EACMS uses the PII to initiate appeals, provide systemic informal resolution and pre-hearing support, federal hearing officers to have case data during appeal hearings for review and update, and to provide data tracking of appeal caseloads, including the reporting of the close-out of appeals.

The types of appeals are described below:

Specifically, for Individual Eligibility Appeals, PII is used for eligibility for advanced payments of the premium tax credit, cost sharing reductions, Medicaid, Children's Health Insurance Program (CHIP), enrollment in a Qualified Health Plan (QHP), and eligibility for an enrollment period, including Special Enrollment Period (SEP), and for the catastrophic coverage provision. Additionally, the failure of an Exchange to provide timely notice is appealable.

Additionally, for Individual Eligibility Appeals, PII is used for eligibility for an exemption from the individual responsibility requirement. Specifically, for Employer appeals, PII is used for appeals from a notice that the employer may be liable for a tax penalty because it has failed to provide affordable, minimum essential coverage to its employees. PII is also used for eligibility for the Small Business Health Options Program (SHOP) Exchange, including both employee and employer eligibility.

If PII is shared, how are the risks of sharing PII mitigated?

PII is only shared within the OPDIV (CMS)

Will the PII from the third-party website or application be maintained by the OPDIV?

Yes

Describe how PII that is used or maintained will be secured:

Physical: This includes multiple physical security measures within data centers. This include 24/7 Security Staff and Physical Access Control System (PACS) using Secure-Card Key Access, Biometric Scanners, and Alarmed Door.

Technical: Data is encrypted at rest and in transit. Storage encryption renders file system unreadable to staff. Systems are configured for logging and all logs are sent to SIEM and monitored by the security team. IDS systems are placed in line for detection of network anomalies. All systems are scanned for vulnerabilities on a weekly basis and patched monthly.

Administrative: Policies and Procedures have been created on securing PII in the DocuSign system. An example of these, there are Security Awareness and Training (SAT) policies, policies on the storage of PII, access control policies are used for login access, policies for following the NARA record retention policy. Also, DocuSign has policies on continuous monitoring of the system and audit log reviews.

What other privacy risks exist and how will they be mitigated?

All information is encrypted via FIPS 140-2 certified TLS 1.2 between DocuSign and CMS
Changes to the Privacy Policy on the DocuSign website will need to be approved by CMS prior to deployment.