US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

09/12/2017

OPDIV:

CMS

Name:

Administrative Simplification Enforcement and Testing Tool

PIA Unique Identifier:

P-7134352-789945

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?

Yes

Identify the operator.

Contractor

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

Describe the purpose of the system.

Administrative Simplification Enforcement Testing Tool Salesforce (ASETT-SF) is a web- based public facing system that was established to manage, track, and process compliance complaints and the CMS Audit Program for the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Affordable Care Act (ACA) administrative simplification provisions. The public may file complaints for potential violations of the adopted standards by HIPAA covered entities which include health plans, health care clearinghouses and health care providers. ASETT-SF's graphical user interface (GUI) enables users to enter information related to alleged violations of the HIPAA/ACA transactions and code sets (TCSs), Unique Identifiers (UIs), Operating Rules regulations, and other HIPAA/ACA enforcement regulations that may be adopted in the future. It also enables documentation, tracking and reporting of data related to HIPAA compliance audits.

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

ASETT-SF collects complaint information for violations of the HIPAA/ACA transactions, code sets, unique identifiers, and operating rules. Complaint information consists of the entity identification for the person filing a complaint, filed against entity's contact information, and the violation description.

The violation/complaint description can include details regarding an alleged violation of the transactions, code sets, unique identifiers and/or operating rules adopted standards.
Certain electronic transaction standards, such as a health care claim, were adopted under the administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). For example, the administrative transactions involve the exchange of information between providers and health plans. The exchange must be compliant with the standard guides adopted by HIPAA. HIPAA also adopted unique identifiers for providers, health plans, and employers to be used in the electronic standard transactions. If an entity or individual suspects a potential violation of the adopted standards they may file a complaint. When filing a complaint, the complainant describes the potential violation. This information is used to investigate the complaint and achieve resolution. The complainant and filed against entity's information consists of name, email address, phone numbers, mailing address and organization name. External users consist of members of the public, private sector, federal, state and local government and internal users of the ASETT- SF system consist of CMS employees and direct contractors. The information collected to gain access to the system is username, password, and security question.

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

ASETT-SF collects complaint information for alleged violations of the HIPAA/ACA transactions, code sets, unique identifiers, and operating rules. Information is collected and stored through the Salesforce cloud service provider that is Fed-Ramp certified. Complaint information consists of the entity identification for the person filing a complaint, filed against entity's identity information, and the alleged violation description. Due to the nature of HIPAA/ACA violations, external users may input PII/PHI information as part of their complaint description or supporting documentation. Access to the ASETT-SF is role based, integrated with the CMS Enterprise Identity Management (EIDM) system. All roles within ASETT-SF consist of Level of Access (LOA) 3 security level. LOA 3 requires multi-factor authentication. Additionally, registered users can only view the information they input into ASETT-SF. Notifications are sent to the complainant to provide confirmation that a complaint was successfully submitted. Letters to the Filed Against Entity describe only the alleged violation, and based on the complainant's preference, the complainant's contact information may be shared as part of the complaint investigation process.
Administrators of ASETT-SF are the only entities that can view complaint information, since they are assigned to facilitate the complaint resolution process. Administrators consist of CMS enforcement experts and direct contractors that work on the behalf of CMS. Currently the Salesforce cloud licenses are purchased from and maintained under contract with Actionet.Inc. In the future licenses will be renewed and maintained under a blanket purchase agreement with the CMS Enterprise Salesforce.

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

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

Patients

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

PII is used to contact entities that are filing a complaint and entities that a complaint has been filed against. The informal voluntary approach to complaint enforcement requires collaboration among the complaint entities on complaint resolution and compliance with the possible development of a corrective action plan (CAP). The external and internal user credentialing information is used to gain access to the system in order to file complaints and for normal system support operations. SORN# 09-70-0544

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

Other than the primary use of PII for entity/ individual involvement in complaint resolution, there are no secondary uses.

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

Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104–191, which was enacted on August 21, 1996.
Through subtitle F of title II of that law, the Congress added to title XI of the Social Security Act a new part C, entitled ‘‘Administrative Simplification.’’ (Public Law 104–191 affects several titles in the United States Code); 5 USC 552 a(e) (1); 45 CFR 164.514 (e); 44
USC.3544; 42 USC 1306.

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.

SORN# 09-70-0544, Health Insurance Portability and Accountability Act (HIPAA) Information

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Hardcopy

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 Information Collection Approval #0938- 0948 Paperwork Reduction Act (PRA). Currently being under review for reinstatement as of 09/13/2016.

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Within HHS

PII is disclosed to, or shared with, Program Management National Standard Group within HHS in order to obtain appropriate contact information and any policy related details that may be relevant for the complaint investigation. PII is disclosed to, or shared with, the Office for Civil Rights (OCR) within the U.S. Federal Government (HHS) in order to share and obtain any information that may be relevant for complaint resolution.

State or Local Agencies

PII is disclosed to, or shared with, a state and/or local government entity during complaint investigation and to obtain any additional information that may be relevant for complaint resolution.

Private Sector

PII is disclosed to, or shared with, a nongovernment entity such as a contractor, a business associate or a non-profit organization. A non-government organization is contracted for administration and maintenance of the ASETT-SF system

Describe any agreements in place that authorizes the information sharing or disclosure.

Current Salesforce licenses are purchased and maintained under contract with Actionet, Inc. In the future, the licenses will be purchased and maintained under a CMS blanket purchase agreement. When the CMS Enterprise Salesforce is in place, an Information Sharing Agreement (ISA) will need to be established.

Describe the procedures for accounting for disclosures.

PII in ASETT-SF is available to state/local agencies and OCR, and outside contractors only if they are parties to a HIPAA complaint, or request specific complaint related information. ASETT-SF rarely shares PII because most of the time when complainants file complaints they request anonymity. When ASETT-SF does share PII information, requests for PII information must be approved and are documented in the notes storage for the specific record. Recorded is the date, name of recipient, address, phone, and reason for the request. We also upload a copy of the information that is sent to the requestor in ASETT-SF secure storage that cannot be accessed without administrative rights.

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

A warning banner is displayed on the ASETT- SF website prior to registration. All individuals (CMS employees, contractors, and external users and registrants) using the ASETT-SF application must accept the Terms and Conditions regarding how their PII is going to be used via privacy practices that are posted on the ASETT-SF website. Also, there is a Privacy Policy footer that states:

“PERSONALLY PROVIDED INFORMATION: The information that is collected is only required for individuals wishing to file a complaint regarding the Health Insurance Portability and Accountability Act (HIPAA) of 1996, regarding all enforceable Administrative Simplification provisions, except for Privacy. If you choose to provide us with additional information about yourself through an e-mail message, or ASETT- SF, we will only maintain the information as long as needed to respond to your question or complaint. However, all communications addressed to the HHS Secretary, or the Webmaster, or the CMS Administrator are maintained, as required by law, for historical purposes. These communications are archived on a monthly basis, but are also protected by the Privacy Act that restricts our use of them, yet permits certain disclosures."

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.

Information is required to conduct enforcement investigation and communicate with complaint entities. Filing complaints and providing information is a voluntary optional process.
When voluntarily filing a complaint, individuals have an option to remain anonymous to the complaint filed against entity. The user can opt out by not accepting the Privacy Terms and Conditions that are posted on the ASETT-SF website. If the external user chooses to opt out, they will not be able to submit a complaint electronically via the ASETT-SF website. A user may opt out and manually file a paper complaint. Internal users of the ASETT-SF system consist of CMS employees, direct contractors. The information collected to gain access to the system is username, password, and security question. A user cannot opt out of providing this information because it is required to perform their job duties.

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

If there are major changes to the ASETT-SF system, individuals will be notified via mail, email, or phone when data use or disclosure changes occur in the system. If the ASETT-SF application is changed the system of record will be modified and a revised Office Management & Budget (OMB) information collection approval will be sought. There is a question in ASETT-SF when a registrant files a new complaint which asks them if it is okay to use their personal information and complaint details during investigation. There is also a privacy statement in ASETT-SF which explains how their data will be used and disclosed; the user must agree to the privacy policy before they can successfully register a complaint. The SORN that is applicable for ASETT-SF is 09-70-0544.

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.

Before an individual registers in the enforcement tool, he or she will see the Privacy notice instructing them of actions for suspected violation. If an individual believes that a covered entity or business associate violated his/her health information privacy rights or committed another violation of the Privacy, Security or Breach Notification Rules, he/she may file a complaint with the Office for Civil Rights (OCR). The individual may also file a HIPPA compliant via email at hipaacomplaint@hhs.gov. An individual can contact the Help Desk for general assistance. To speak with a Helpdesk representative, call (703) 951- 6810. Email inquiries can be sent to asett@actionet. com. The reported issue will be resolved as necessary and a response will be sent to the entity.

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

As part of the complaint investigation and resolution process employed by ASETT-SF, there are monthly periodic reviews to ensure that users don't have elevated privileges, user accounts are terminated if they are no longer employed on the ASETT-SF contract, along with reviewing log files for configuration changes, errors, and anomalies to ensure confidentiality, integrity, and accuracy.

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

Users:

ASETT-SF access is needed to file HIPAA complaints. User credentials and complaint information are accessed by the user to update credential information and upload complaint documentation such as test files, correspondence and relevant reports.

Administrators:

ASETT-SF access is needed by Administrators to process HIPAA complaints and manage resolution. Administrator access is used to contact complainants and complaints filed against entities to investigate complaints, request additional complaint information and coordinate complaint resolution or corrective action for compliance.

Developers:

ASETT-SF access is required by developers for evaluating, testing and completing system maintenance and enhancements.

Contractors:

ASETT -SF access is needed by direct contractors to meet contract requirements for system operations, maintenance, reporting and complaint administration and management.

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

Access to the ASETT-SF has multi-factor authentication through Salesforce until the system has been integrated with the CMS Enterprise Identity Management system (EIDM). Access to PII is assigned by the administrator based on the duties ranging from no access to privileged access for the administrator and system maintainer that are responsible for maintaining the system. ASETT-SF has system specific rules of behavior (ROB) that are documented and include a description for each type of user: users, developers, system administrator and database administrator that minimize access to information based on their need to know.

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 system is configured so that a complainant can only see their own information. The administrator has established access controls for individuals which are based on their assigned duties.

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.

Training includes annual CMS Computer-based Privacy and Awareness training.

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

Insider threat training. Role-based system security training is provided for specific individuals, routinely and as needed.

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 HIPAA Information Tracking System (HITS) (a sub-system of ASETT-SF) maintains complaint data for tracking HIPAA complaint/compliance enforcement and reports. DISPOSPITON: Temporary. Destroy/delete 6 years after the CY in which the case is closed (includes complaints, compliance reviews and any other entries). Records are maintained according to NARA Disposition Authority: N1-440-09-2.

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

ASETT-SF applies the principle of least privilege as well as a role based view on granting rights. All access is requested and approved before being granted. All Production access requires Program Manager approval. Each user is assigned a Role and each Role's rights are restricted to only the data and server resources needed to perform their job.
Registrants must go through an identity proofing process in order for he/she to obtain a user name and password for utilizing the ASETT-SF system and submitting a complaint. New ASETT-SF team members are processed through an on boarding process that defines their role and access information. ASETT-SF has system specific rules of behavior (ROB) that are documented and Include a description for each type of user: users, developers, system administrator and database administrator. The system and data center are located in a physically secure area that includes controlled physical access to the building with security guards which are responsible for the physical access of the data center. Access to the building is controlled with the use of personal security access badges. There is also video monitoring of the data center. Firewalls separate the presentation, application, and data zones. Intrusion detection devices are installed on the network to detect malicious activity.

Identify the publicly-available URL:

https://asett.cms.gov

This web address may not be operation as it is not ready to go live at this time.

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Session Cookies that do not collect PII.

Does the website have any information or pages directed at children under the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

null