

Date Signed: 11/4/2022

Acronyms

ATO - Authorization to Operate
 CAC - Common Access Card
 FISMA - Federal Information Security Management Act
 ISA - Information Sharing Agreement
 HHS - Department of Health and Human Services
 MOU - Memorandum of Understanding
 NARA - National Archives and Record Administration
 OMB - Office of Management and Budget
 PIA - Privacy Impact Assessment
 PII - Personally Identifiable Information
 POC - Point of Contact
 PTA - Privacy Threshold Assessment
 SORN - System of Records Notice
 SSN - Social Security Number
 URL - Uniform Resource Locator

General Information

Status:	Approved	PIA ID:	1509301
PIA Name:	OS - ECAPE - QTR3 - 2022 - OS1238046	Title:	Electronic Case Adjudication and Processing Environment
OpDiv:	OS		

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	Increased the Oracle database table structure from small to large, that has helped us in significant database size reduction. No other changes.
PTA - 3:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA - 5:	List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored.	ECAPE collects and maintains Personally Identifiable Information (PII) in order to record and adjudicate appeals of Medicare claims and services in dispute. To initiate and then to

adjudicate the appeal, ECAPE retrieves and stores information from the CMS MAS related to the appeal, including previous appeal case data (legal documents which may contain medical evidence), beneficiary enrollment data, appellant information, and claim information. The types of information that is collected, stored and later transmitted back to CMS includes: contact phone numbers, email addresses, street addresses, appellant name(s), beneficiary name(s), dates of birth (DOBs), Appellant or Representative name(s), physician name(s), Social Security Numbers (SSNs), Tax Payer Identification Numbers, Financial Account Information, Employment Status, Medical Record Numbers (MRNs), Medicare Beneficiary Identifier (MBI) and Health Insurance Claim Numbers (HICN). It also collects and maintains other pertinent evidence (not submitted in previous appeals), and employee AMS/ECAPE user credentials. Other pertinent medical evidence may include written test results, medical notes, prescriptions, letters for the record, electrocardiograms (EKGs), treatments, x-rays, justification for medical need, etc. Although OMHA does not solicit additional evidence, additional information is often supplied by the appellant and/or their representatives, which is incorporated into the case file and may be used to process the appeal. Since Health and Human Services (HHS) does not request the supplemental information, the appellant and/or their representative determines what will be sent as additional evidence. This information can be any type of information that is somehow related to the case and that the appellant, or their representative, deems as an important component of information relevant to the appeal. ECAPE receives submission of this additional information from either the existing paper Request for Hearing (RFH) form submitted by appellants, by supplemental submissions on paper or on compact disc (CD)/digital video disc (DVD), or by electronic data entry of the RFH information via the ECAPE e-Appeals Portal. Appellant submissions of additional information and data to the ECAPE e-Appeals Portal is purely voluntary. However, in certain cases, the lack of such information could adversely impact the resolution of an appeal. Types of information submitted to the portal vary based on the facts of the appeal. These can include, but are not limited to, financial information, additional medical evidence, medical notes, medical record numbers, treatment details, expert opinions, employment, and/or work related information, etc. Once a final disposition is reached, all of the Level 3 appeal case data compiled is then transmitted back to the CMS MAS system. This transmittal may include new data which may have been acquired from the appellant during the adjudication process. ECAPE is only accessible by OMHA personnel and contractors. OMHA personnel credentials are established and maintained by the HHS AMS with a temporal copy stored in ECAPE. OMHA contracted technical personnel have access to ECAPE to maintain its operation and support modifications; their credentials are stored in ECAPE. All

information is stored for seven years.

PTA - 6:

Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual.

ECAPE supports the end-to-end business process for the adjudication of Medicare claim appeals by the OMHA ALJs. ECAPE retrieves and stores MAS data only for a specific appeal in addition to (and upon receipt of) collecting and storing data via a RFH to adjudicate the appeals. ECAPE collects and maintains the following PII in order to record and adjudicate appeals of Medicare claims and services in dispute. The type of information includes contact phone numbers, email addresses, street addresses, appellant name(s), beneficiary name(s), DOBs, Appellant or Representative name(s), physician name(s), SSNs, MRNs, MBI, HICN, and other pertinent evidence (not submitted in previous appeals). The system also maintains the ALJ working case file that may include administrative records and legal documents (such as, ALJ notes, case analyses, attorney work product, recordings, RFH, notices, decisions, exhibit lists, responses, instructional sheets, and post adjudicative materials). The system also stores other pertinent medical evidence that may include written test results, medical notes, prescriptions, letters for the record, EKGs, treatments, x-rays, justification for medical need, etc. Although OMHA does not ask for the additional evidence, this information is often supplied by the appellant and is typically used to process the appeal. ECAPE receives other pertinent information from either the existing paper RFH form submitted by appellants, by supplemental submissions on paper or on compact disc (CD)/digital video disc (DVD), or by electronic data entry of the RFH information via the ECAPE web portal. Submission of this information and data is purely voluntary. However, the lack of such information could adversely impact the resolution of the appeal. The system also maintains employee AMS/ECAPE user credentials. The primary source of the data stored in ECAPE is acquired from the CMS MAS. The other source of ECAPE data comes from either the paper submissions by appellants and/or the ECAPE e-Appeal Portal, as described above. The ECAPE system retrieves data electronically from MAS once OMHA receives an RFH. ECAPE is only accessible by OMHA personnel and contractors. OMHA personnel credentials are established and maintained by the HHS AMS with a temporal copy stored in ECAPE. OMHA contracted technical personnel have access to ECAPE to maintain its operation and support modifications; their credentials are stored in ECAPE. The ECAPE e-Appeal Portal will be accessible by all members of the public to file a request for a hearing and to transmit supplemental information and evidence to support their appeal. Once the appeal is finalized and adjudicated, OMHA shares back with CMS MAS system an updated version of the appeals file, which would include any additional information captured by ECAPE during the course of the appeal process.

PTA - 7:

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

Yes

PTA - 7A:	Does this include Sensitive PII as defined by HHS?	Yes
PTA - 8:	Does the system include a website or online application?	Yes
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	Yes
PTA - 9:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	ECAPE automates several aspects of OMHA's business process, especially in the areas of managing and handling documents, case processing workflow, generating correspondence, scheduling and managing hearings, supporting the decision process, management information and providing a public portal for appellants to file an appeal and submit evidence. Appellant's use the website/portal to request medical appeals and provide the required information documents required for the appeal.
PTA - 10:	Does the website have a posted privacy notice?	Yes
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA - 12:	Does the website use web measurement and customization technology?	No
PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA - 14:	Does the system have a mobile application?	No
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	No
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	<ul style="list-style-type: none"> Social Security Number Mother Maiden Name Taxpayer ID Legal Documents User Credentials Driver License Number Truncated SSN Email Address Date of Birth Mailing Address Name Phone numbers Military Status Medical Records Number Employment Status Medical records (PHI)
-----------------	---	---

		Financial Account Info Other - Free text Field - Medicare Beneficiary ID, Health Insurance Claim Number, and Medical Notes.
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Business Partners/Contacts (Federal, state, local agencies) Employees/ HHS Direct Contractors Grantees Patients Members of the public Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	501 - 2000
PIA - 4:	For what primary purpose is the PII used?	PII is used for the adjudication of Medical Appeals.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	PII is not being used for secondary purposes.
PIA - 6:	Describe the function of the SSN and/or Taxpayer ID.	The SSN currently serves as the unique identifier for Medicare beneficiaries. The SSN is a part of the Health Insurance Claim Number (HICN) which is Medicare beneficiary's identification number submitted in the request for hearings and used by Office of Medicare Hearings and Appeals (OMHA) to uniquely identify claimants who are a party to the appeal. The SSN may appear in other parts of the case file due to the variety of documents that can be incorporated into the case file depending on the facts and the complexity of the case.
PIA - 6A:	Cite the legal authority to use the SSN.	The collection and use of the SSN information is authorized by the Social Security Act (section 1155 of Title XI and sections 1852(g)(5), 1860D-4(h)(1), 1869(b)(1), and 1876 of Title XVIII), 42 CFR 405.1014 also describes the requirement to collect the HICN.
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	Authority for this system is given under 205 of Title II, 1155 and 1156 of Title XI, 1812, 1814, 1816, 1842, 1869, and 1872 of Title XVIII of the Social Security Act (the Act), as amended (42 United States Code (U.S.C.) sections 405, 1320c-4, 1320c-5, 1395d, 1395f, 1395h, 1395u, 1395ff, and 1395ii). Additional authority for this system is given under Title IX, Subtitle D of the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (Public Law (Pub. L.)
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	Records are retrieved by Name, SSN, and Medical Appeal Case number.
PIA - 8B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	File SORN 09-90-1501 MAS system of records notice (SORN) 09-70-0566

PIA - 9:	Identify the sources of PII in the system.	<p>Directly from an individual about whom the information pertains</p> <ul style="list-style-type: none"> In-person Hard Copy Mail/Fax Phone Email Online <p>Government Sources</p> <ul style="list-style-type: none"> Within the OPDIV Other HHS OPDIV State/Local/Tribal Other Federal Entities <p>Non-Government Sources</p> <ul style="list-style-type: none"> Members of the Public Public Media/Internet Private Sector
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 10C:	Explain why an OMB information collection approval number is not required.	A Request For Hearing (RFH) comes from beneficiaries, patients, and the public and these contain PII. Electronic Case Appeal and Processing Environment (ECAPE) maintains and stores whatever the public provides Office of Medicare Hearing and Appeals (OMHA) on their RFHs. The Office of Management and Budget (OMB) information and collection approval number is non-applicable to OMHA since OMHA is exempt under the Paperwork Reduction Act Of 1995 Statutory Exemption 44 U.S.C. 3518(c) (5 CFR 1320.4).
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	Yes
PIA - 11A:	Identify with whom the PII is shared or disclosed.	<ul style="list-style-type: none"> Other Federal Agency/Agencies Private Sector State or Local Agency/Agencies
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	An Information Security Agreement (ISA) is in place between Office of Medical Hearings and Appeals (OMHA) and Center for Medicare/Medicaid Services (CMS), the owner of the Medical Appeals System (MAS). Procedures for accounting for disclosures is provided in the MAS SORN (09-70-0566). Disclosure of MAS information to OMHA/ECAPE will only be to the extent necessary to adjudicate Level 3 appeal requests. If an authorization for the disclosure has been obtained from the data subject, then no routine use is needed. The Privacy Act allows for disclosures with the prior written consent of the data.

PIA - 11C:	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	An information Security Agreement (ISA) is in place between OMHA and CMS.
PIA - 11D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	Primary roles have been created as a part of the ECAPE system. Each User is assigned a role, or roles to that control access to the Appeals

system. A complete list of Access Control privilege's in managed in the HHS ECAPE Create/Read/Update/Delete/Assignments/Search (CRUDAS) spreadsheet.

ECAPE only allows access to Privacy Act data to OMHA employees and contractor staff performing ECAPE operational support. ECAPE does not provide access to Privacy Act information outside of HHS or ECAPE support contractors. ECAPE contractor's contracts include Office of the Chief Information Officer (OCIO) approved language for the protection of PII/Personal Health Information (PHI).

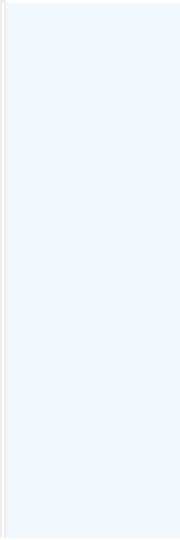
ECAPE adjudicatory team user's send notices and other appeals documents to appeal parties as part of the appeal adjudicatory process as in accordance with (IAW) applicable laws governing the Medicare appeals process. Providing PII/PHI to parties of an appeal as part of the appeal adjudication process is authorized by § 205 of Title II, §§ 1155 and 1156 of Title XI, §§ 1812, 1814, 1816, 1842, 1869, and 1872 of Title XVIII of the Social Security Act (the Act), as amended (42 United States Code (U.S.C.) sections 405, 1320c-4, 1320c-5, 1395d, 1395f, 1395h, 1395u, 1395ff, and 1395ii). Additional authority for this system is given under Title IX, Subtitle D of the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (Public Law (Pub. L.) 108-173).

This is controlled by the OMHA Case Processing Manual (OCPM) and Chief Judge Bulletin (CJB) 17-002 on handling of PII. The CJB defines PII, outlines the duty of all OMHA employees and contractors with regard to PII, explains how OMHA employees and contractors protect PII in the workplace and while teleworking (if applicable), provides the breach notification protocol in the event of an actual or suspected breach, and outlines penalties associated with violation of the Privacy Act and regulations. The OCPM details procedures for contact with appeal parties in general and refers employees to the CJB for PII aspects. All contact with appeal parties and a record of what was provided is logged in ECAPE by the adjudicatory staff.

For external data requests not related to the adjudication of an appeal, OMHA Appeals Policy and Operations Division (APOD) manages those requests as required by Chief Judge Bulletin and logs any PII/PHI provided outside HHS.

PIA - 13:	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	Individuals wishing to 'opt-out' of the collection or use of their PII by MAS should contact the MAS system manager as described in the MAS SORN (09-70-0566).
PIA - 14:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). Alternatively, describe why they cannot be notified or have their consent obtained.	Individuals would be notified directly of major system changes that affect their rights or interests, but no such changes are anticipated. Major changes would also be reflected by updates to the SORN.
PIA - 15:	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 no process exists, explain why not.	The subject individual should contact the CMS Privacy Office, and reasonably identify the records and specify the information to be contested. In addition the individual should state the corrective action sought and the reasons for the correction with supporting justification. These Procedures are in accordance with Department regulation 45 CFR 5b.7.
PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not.	OMHA employs a disciplined change management process, which includes OMHA appeal processing experts and senior management, to periodically review the entire ECAPE system and its PII data requirements. Additionally, the integrity and accuracy of the PII in the ECAPE system is reviewed as part of OMHA's adjudication process. OMHA staff reviews the information, which includes PII as described above, for each appeal during the adjudication process.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA - 17A:	Select the type of contractor.	Grantees HHS/OpDiv Direct Contractors Third-Party Contractor (Contractors other than HHS Direct Contractors)
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA - 18:	Provide the reason why each of the groups identified in PIA- 17 needs access to PII.	OMHA employs the principle of least privilege, allowing only authorized accesses for which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. The groups listed have key roles in the support of the Medical Appeals system.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	OMHA has written procedures based on system requirements that identify specific roles which require PII access along with the appropriate level of access.

<p>PIA - 20:</p>	<p>Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.</p>	<p>ECAPE includes role based security and access control built into the system.</p>
<p>PIA - 21:</p>	<p>Identify the general security and privacy awareness training provided to system users (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.</p>	<p>OMHA personnel and contractors are required to complete the yearly mandatory HHS Annual Privacy and Security Training.</p>
<p>PIA - 22:</p>	<p>Describe the training system users receive (above and beyond general security and privacy awareness training).</p>	<p>HHS' Annual Privacy and Security training courses are comprehensive courses that are reviewed and updated annually by HHS, and are deemed to cover all of OMHA's needs regarding the ECAPE system.</p>
<p>PIA - 23:</p>	<p>Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).</p>	<p>ECAPE System Of Record (SORN) No. 09-90-1501 entitled "Administrative Law Judge (ALJ) Working File, Office of Medicare Hearings and Appeals," to cover OMHA ALJ working files previously maintained as part of the Social Security Administration's (SSA) ALJ Working File system of records 60-0005 (last published at 74 FR 19617). The working files covered under new System of Records Notice (SORN) 09-90-1501 are created and used by OMHA ALJs and members of their staffs for internal purposes, to document actions taken by OMHA at the hearing level in each Medicare appeal case that OMHA reviews. The working files are separate from the official case files, which are covered under other SORNs (<i>i.e.</i>, HHS SORN 09-70-0566 covers case files on Medicare claims appeals, and SSA SORN 60-0089 covers case files on Medicare entitlement appeals).</p> <p>The Working File Retention Schedule is the NARA-approved records control schedule RG-0468: Health and Human Services, General Records of the Department of and Disposition Authority DAA-0468-2012-0003 - 3 Years after the Level 3 appeal is closed. Electronic working file documents are deleted per that Disposition Authority. The appeal official case file is transferred to Center of Medicare and Medicaid Services (CMS) Appeals system and managed per that system's SORN and disposition authority.</p>
<p>PIA - 24:</p>	<p>Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.</p>	<p>Security measures are designed into the system according to National Institute of Standards and Technology (NIST) 800-53 Revision (REV) 4.</p>



Implementation of controls is organized on a risk based model and all administrative, physical and technical controls are reviewed annually. The cloud service provider hosting ECAPE has been Federal Risk and Authorization Management Program (Fed Ramp) certified to NIST 800-53 REV 4 requirements. PII is protected using administrative, technical and physical security controls. Administrative controls include limited access to PII to those OMHA users based on their role in adjudicating appeals. Technical controls include two factor authentication for OMHA users to access PII in the system. Physical controls include limiting physical access to the system's equipment in the data center to those individuals approved and authorized by the cloud service provider to gain physical access.