

General Information

PTA / PIA Name:	OS - AWRS - QTR2 - 2026 - OS3505329	PTA / PIA ID:	4566700
Component Name:	OS - Anata Web Redaction Suite	ATO Boundary Name:	Anata AI Redaction Suite
Overall Status:	Complete 	# of Days - Open:	29
Submitter:		Submit Date:	6/24/2026
Next Assessment Date:	07/01/2029	Expiration Date:	7/1/2029
Office:		OpDiv:	OS
Security Categorization:	Not Rated		
Make PIA available to Public?:	No	PIA Required:	Yes
General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Test	
General 02:	Is this a FISMA-Reportable system?	No	
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes	
General 04:	ATO Date or Planned ATO Date.		
General 05:	Is the system or electronic information collection, agency or contractor operated?		
History Log:	View History Log		

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Arianne Perkins
PTA 01A:	POC Title and Organization	Director, FOIA/PA Division OS/ASPA
PTA 01B:	POC Email Address	arianne.perkins@hhs.gov
PTA 01C:	POC Phone Number	202-841-2789
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
PTA 03:	Is the data contained in the system owned by the agency or contractor?	Both

PTA 04:

Please give a brief overview of the purpose of the system by describing what the functions of the system are and how the system carries out those functions in support of HHS.

The Anata Artificial Intelligence (AI) Redaction Suite is an AI-powered document review and redaction system designed for processing government documents, particularly for Freedom of Information Act (FOIA) requests.

The suite's capabilities include:

1. Identifying and redacting sensitive information such as personally identifiable information (PII), protected health information (PHI), and law-enforcement-sensitive data.
2. Using large language models (LLMs) and semantic analysis rather than relying solely on keyword matching or regular expressions.
3. Supporting FOIA exemption workflows by helping agencies determine what information should be withheld before public release.
4. Reducing the manual effort involved in reviewing large document collections.

The system will support the Department of Health and Human Services (HHS) Freedom of Information Act (FOIA) office by using the AI suite to recommend potential redactions for human review. Authorized users review, propose, edit, and finalize redactions before the system applies them to records prepared for HHS FOIA release. The AI tool(s) will not be trained using PII collected in the system.

PTA 05:

List and/or describe all the types of information that are collected, maintained, and/or shared by the system regardless of whether that information is PII and how long that information is stored.

The system collects and maintains limited user account and access information including name, HHS email address, role, authentication, information managed through HHS Entra ID, and audit activity.

The system also processes HHS-provided records, case or request information, document metadata, redactions, redaction recommendations, reviewer edits, finalized redactions, redacted output files and system logs. PII (personally identifiable information) may be included in source records, related metadata, and internal redaction/compliance logs, including where exact redacted text is captured; these logs are retained for 18 months. Logs transmitted to HHS's event hub and HHS Splunk are action-based and do not include exact redacted text. Other information is retained in accordance with applicable HHS and NARA retention policies and system security requirements.

PII may include:

Social Security Number

- Alien registration number
- Employee ID number
- Criminal records
- Video or Audio Identifiers or Recordings
- Mother Maiden Name
- Certificates
- Taxpayer ID
- Vehicle Identifiers
- Legal Documents
- User Credentials
- Driver License Number
- Truncated SSN
- Email Address
- Education Records
- Date of Birth
- Mailing Address
- Devices Identifiers
- Patient ID Number
- Name
- Phone Numbers
- Military Status
- Photographic Identifiers
- Medical Records Number
- Employment Status
- Foreign Activities
- Biometric Identifiers
- Financial Account Info
- Passport Number
- Others - Chart No.,TIN, DUNS, Provider Licence #
- Other - Free text Field: Otherwise provided by HHS

PTA 05A: Are user credentials used to access the system?

Yes

PTA 05B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS Email Address Password
PTA 06:	Describe why each type of information is collected, maintained, and/or shared by the system. Specify what information is collected about each category of individual.	There are two main categories of individuals the PII is being collected from: Individuals appearing within source records: - The system does not solicit information from these individuals. Their PII is contained in HHS-provided records submitted to the system for FOIA review and redaction, and is processed only for that purpose: identifying, reviewing, and applying or removing redactions before disclosure. The specific PII varies by record and is not determined by the system. It may include any PII present in the source documents, such as names, contact information, identifiers, account or case numbers, dates, and substantive case content. - Sub-categories of individuals whose information may appear include members of the public, FOIA requesters, complainants, beneficiaries, patients, business contacts, HHS personnel, other government personnel, contractors, and other individuals identified in the source records. This information is maintained only for the duration required to process the FOIA request and is dispositioned under the applicable National Archives and Records Act (NARA) schedule. It is shared only as part of the FOIA response, consistent with applicable exemptions and HHS disclosure procedures. Sharing of information is at the discretion of HHS. Authorized system users: - The system maintains limited PII about the staff and contractors who operate it, specifically name, HHS email address, assigned role, and audit activity. This information is collected and maintained for access management, role-based authorization, and audit logging. It is not shared externally and is used solely to control and record system access.
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	Yes
PTA 08A:	Provide the URL(s).	portal.foia.hhs.gov
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	No

PTA 09:	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.	The application supports authorized legal reviewers in reviewing, accepting, entering, and updating redactions for records prepared for FOIA release. Access is limited to cleared legal reviewers using government-furnished equipment (GFE). Users access the website through HHS-approved remote access using Palo Alto Networks Prisma Access/GlobalProtect Virtual Private Network and authenticate using HHS Entra ID.
PTA 10:	Does the website have a posted privacy notice?	No
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?	Yes
PTA 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	Session Cookies- Does Not Collect PII Other technology - Does Not Collect PII
PTA 12B:	What other technology is used?	In order to help developers diagnose and fix bugs, Anata monitors application errors and performance issues, records around 10% of user sessions for replay analysis, and records 100% of sessions where errors occur. In order to maintain the user experience across sessions, the website stores user preferences, remembers search filters and browsing state, and maintains collection and document viewing preferences. All logging is done through Azure's Log Analytic Workgroups.
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:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	Yes
PTA 21A:	What are the AI tools and how are they used?	The known Artificial Intelligence (AI) use case is in analyzing records and making suggestions as to what parts of the record should be redacted, under which FOIA exemption, based on the context of the document, and HHS guidance. The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks. The AI tool(s) will not be trained using PII collected in the system.

Privacy Impact Assessment

Privacy Impact Assessment

PIA 22:

Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.

Identifying Numbers

Social Security Number

Truncated SSN

Alien Registration Number (A-number)

Taxpayer ID Number (TIN)

Driver's License Number

Passport Number

Employee ID Number

Healthcare Provider License # (e.g., NPI)

Financial Account Information (e.g., account numbers, credit card numbers)

Device Identifiers

Vehicle Identifiers (e.g., VIN, license plate number)

DUNS

Biographical Information

Name

Date of Birth

User Credentials

Mother Maiden Name

Certificates (e.g., training certificates)

Criminal Records

Education Records

Employment Status/History

Foreign Activities

Legal Documents

Military Status/History

Contact Information

Email Address (Personal)

Mailing Address (Personal)

Phone Numbers (Personal)

Email Address (Business)

Mailing Address (Business)

Phone Numbers (Business)

Biometrics/Distinguishing Features

Photographic Identifiers

Video or Audio Identifiers or Recordings

Medical Information

Medical Records

Medical Records Number

Patient ID Number

Other

Other

PIA 22A:	Identify the “other” type(s) of personally identifiable information (PII) not mentioned in the above list.	Chart No.,TIN, DUNS, Provider License #
PIA 23:	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 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	1,000,000 or more
PIA 25:	For what primary purpose is the PII used?	PII is used to support FOIA review, redaction processing, and compliance logging. The system processes PII in HHS-provided records to identify information that may require redaction, allow authorized reviewers to review and edit proposed redactions, prepare redacted records for HHS release processing, and maintain an audit record of redaction actions taken.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	The PII will be used as test data to evaluate the accuracy, efficiency, and reliability of AI-based tools for identifying and suggesting which FOIA exemptions to be applied to redactions.
PIA 27:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID. If the Taxpayer IDs collected are only for businesses include that in your response.	The system does not collect SSNs, truncated SSNs, or Taxpayer IDs as separate data fields or use them as identifiers. These identifiers may be present in HHS-provided records processed for FOIA review. When present, they are processed only to support AI-assisted redaction recommendations, reviewer confirmation or editing of redactions, compliance logging of redaction actions, and preparation of redacted records for HHS release processing. These identifiers may be stored in internal redaction/compliance logs if included in the exact text redacted.
PIA 27A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID. If the Taxpayer IDs collected are only for businesses, you may respond N/A.	The system does not collect or use SSNs, truncated SSNs, or Taxpayer IDs as identifiers or separate data fields. These identifiers may be processed only when present in HHS-provided records reviewed under the Freedom of Information Act, 5 U.S.C. § 552, and HHS FOIA regulations at 45 C.F.R. Part 5, for the limited purpose of FOIA review and redaction.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	Information use and disclosure are governed by the Freedom of Information Act, 5 U.S.C. § 552, and HHS FOIA regulations at 45 C.F.R. Part 5. To the extent records contain information about individuals, use and disclosure may also be governed by the Privacy Act of 1974, 5 U.S.C. § 552a, and applicable HHS privacy, security, records management, cloud service, and AI service requirements.

PIA 29:	Are records in the system retrieved by one or more PII data elements?	No
PIA 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains - Hard Copy Mail/Fax - Email - Online Government Sources - Within the OPDIV - Other HHS OPDIV - State/Local/Tribal - Foreign - Other Federal Entities Non-Government Sources - Members of the Public - Commercial Data Broker - Public Media/Internet - Private Sector
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA 31B:	Explain why an OMB information collection approval number is not required.	An OMB information collection approval number is not required. Under the Paperwork Reduction Act (44 U.S.C. 3501 et seq.; 5 CFR 1320.3(c)), an OMB control number applies only when an agency solicits information from the public by posing identical questions to, or imposing reporting or recordkeeping requirements on, 10 or more persons. The system does not do this. The PII referenced in PIA-23, including PII about members of the public, is contained within HHS-provided source records that the system processes for FOIA review. That PII is received as the content of records already in agency custody, not solicited from individuals through a form, survey, or questionnaire. Processing PII that resides in existing records is distinct from a Paperwork Reduction Act collection of information, so no OMB control number is required.
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	No
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Voluntary

PIA 34:	Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why.	Individuals whose PII appears in HHS-provided records do not submit information directly to the system, so the system does not provide direct notice or obtain consent from those individuals. Any applicable notice or consent for those records is handled by HHS through its original collection, records management, Privacy Act, and FOIA processes. Authorized users request or are approved for access to this internal tool on HHS-approved devices within the HHS network. Anata does not provide a separate consent process for authorized users because the system relies on existing HHS Microsoft Entra ID account information, such as name and HHS email address, only to provision access, authenticate users, manage permissions, and support audit/security functions.
PIA 35:	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). If they cannot be notified or have their consent obtained, explain why.	The system is used internally to process HHS records for FOIA review and redaction under the Freedom of Information Act, 5 U.S.C. § 552, and applicable HHS FOIA processes. Individuals whose PII appears in HHS-provided records do not interact directly with the system, so the system does not provide direct notice or obtain consent from those individuals. Any required notice, consent, or disclosure determination related to the records is handled by HHS. For authorized platform users, limited user information is used only to provision access, authenticate users, manage permissions, and support audit and security functions. We will notify the users by email if anything changes.
PIA 36:	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.	Individuals with concerns about PII in HHS-provided records would use HHS's established Privacy Act, FOIA, privacy, records, or information security processes to submit a request, complaint, or correction inquiry. HHS is responsible for reviewing and resolving those concerns because HHS owns the records, determines any disclosure, and controls any correction or response process. The system is used internally to support FOIA review and redaction, and Anata does not independently release records or make final disclosure determinations. For authorized system users, account and access information is derived from existing HHS Microsoft Entra ID and HHS access processes; any concerns about user account information, access, or audit records would be handled through HHS identity, access management, help desk, or security processes.

PIA 37:	Describe the process in place for periodic reviews of the system to ensure the integrity, availability, accuracy, and relevancy of the PII in the system. Please address each element in your response. If no processes are in place, explain why not.	The system is used internally to support FOIA review and redaction of HHS-provided records. HHS remains responsible for the integrity, accuracy, and relevancy of the underlying source records. The system maintains internal logs of AI-assisted redaction recommendations and reviewer actions, which may include exact redacted text and associated PII. Logs transmitted to HHS's event hub and HHS Splunk are action-based and do not include exact redacted text. Authorized user access is managed through HHS Microsoft Entra ID, and system integrity and availability are supported through access controls, audit logging, monitoring, security reviews, and applicable HHS security requirements.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA 38A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA 38B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Authorized legal review personnel need access to records containing PII to support FOIA review, evaluate AI-generated redaction recommendations, apply or edit redactions, and prepare records for HHS review or release processing. Authorized HHS personnel need access to oversee FOIA processing, review redactions, make final disclosure and release determinations, administer the system, and support security, monitoring, and audit requirements.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Access to PII is limited to authorized users with a need to know. Users must complete applicable HHS clearance, onboarding, and access approval requirements before access is granted. Access is provisioned and scoped through HHS Entra ID role-based access controls (RBAC).
PIA 41:	Describe the technical methods in place to allow those with access to PII to access only the minimum amount of information necessary to perform their job.	Access is limited through HHS Entra ID role-based access controls (RBAC), authentication, and approved user provisioning. Authorized reviewers are granted access only to the records needed for their assigned FOIA review work. Because reviewers must evaluate the full content of assigned records to identify information requiring redaction, access to PII within those assigned records is necessary to perform their duties.
PIA 42:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) to make them aware of their responsibilities for protecting the information being collected and maintained.	All system users receive mandatory HHS security and privacy awareness training.

PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	System users receive role-specific training on system procedures. After onboarding, users also receive system training on how to access and use the application. Anata HHS contractors receive additional training and guidance relevant to their system support and review responsibilities. System engineers receive additional technical training relevant to system administration, security operations, and protection of system data.
PIA 44:	Describe the process and guidelines in place for the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	HHS FOIA case files follow NARA General Records Schedule (GRS) 4.2: Information Access and Protection Records, item 020, "Access and disclosure request files" (Disposition Authority DAA-GRS-2016-0002-0001). The recordkeeping copy is temporary, destroyed 6 years after final agency action or 3 years after final adjudication by the courts, whichever is later. Transitory and intermediary processing artifacts (extracted text, embeddings, and short-lived working copies not kept as the official record) follow GRS 5.2: Transitory and Intermediary Records, item 010 (DAA-GRS-2022-0009-0002) for transitory records and item 020 for intermediary copies.

PIA 45:

Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.

Administrative:

Access to the system is governed by Microsoft Entra ID role assignment. Users must be explicitly granted a given role by a tenant administrator before they can authenticate; unassigned users are denied at the platform edge. Each service component runs under its own scoped Managed Identity, enforcing least privilege between workloads. All code and infrastructure changes flow through pull-request review and Continuous Integration (CI) validation before deployment. The team conducts periodic security audits and maintains the findings, remediation status, and architectural decisions.

Technical:

Authentication is handled by Entra ID. After five failed attempts within five minutes, the account is locked for fifteen minutes. Browser sessions are terminated after fifteen minutes of inactivity. All traffic is encrypted in transit using Transport Layer Security (TLS) 1.2 or higher, including mutual TLS between internal services. All data at rest — documents, database records, and editor state — is encrypted using Azure-managed Advanced Encryption Standard with 256-bit keys (AES-256), with double encryption on blob storage. No credentials reside in source code; all secrets are stored in Azure Key Vault and retrieved at runtime via Managed Identity. The system operates entirely within a private virtual network with no public ingress; user access requires the agency VPN. File uploads are validated by extension, size, and binary signature, and filenames are sanitized. Every security-relevant event — authentication outcomes, authorization denials, document access, redaction changes, and administrative actions — is logged in structured form with a unique request identifier for end-to-end correlation.

Physical:

The system is hosted exclusively in the HHS Microsoft Azure tenant; no on-premises components, local databases, or user-managed hardware process PII. Data is geo-redundantly backed up but remains within Azure's controlled infrastructure at all times. The application supports no removable-media workflows.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	Privacy Analyst Review Date:	6/24/2026
Privacy Analyst Review Comments:	This PIA is ready for your review. All necessary questions have been answered. Thank you, Jon	# of Days - PA Review:	0

SOP Review

SOP Review Decision:	Approved	SOP Review Date:	6/24/2026
SOP Review Comments:		# of Days - SOP Review:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	Agency Privacy Analyst Review Date:	6/25/2026
Agency Privacy Analyst Review Comments:	Reviewer: Godisgreat Peters 6/25/2026 All comments have been addressed, this PIA is ready for SAOP review and approval. Please see comments and update accordingly: PTA-4: Revised your response to read "The Anata Artificial Intelligence (AI) Redaction Suite is an AI-powered document review and redaction system designed for processing government documents, particularly for Freedom of Information Act (FOIA) requests. The suite's capabilities include: 1. Identifying and redacting sensitive information such as personally identifiable information (PII), protected health information (PHI), and law-enforcement-sensitive data. 2. Using large language models (LLMs) and semantic analysis rather than relying solely on keyword matching or regular expressions. 3. Supporting FOIA exemption workflows by helping agencies determine what information should be withheld before public release. 4. Reducing the manual effort involved in reviewing large document collections. The system will support the Department of Health and Human Services (HHS) Freedom of Information Act (FOIA) office by using the AI suite to recommend potential redactions for human review. Authorized users review, propose, edit, and finalize redactions before the system applies them to records prepared for HHS FOIA release. The AI tool(s) will not be trained using PII collected in the system. " PTA-5: Per PIA 22, please include the following PII "Alien registration number, Employee ID Number, Criminal records, Video or Audio Identifiers or Recordings."	# of Days - APA Review:	1

SAOP Review

SAOP Review
Decision:

Approved

SAOP Review
Comments:

SAOP Review
Date:

7/2/2026

of Days - SAOP
Review:

7

SAOP Signature

Date	User	Type	Name	Original Value	New Value
7/2/2026 2:42 PM	BAUR, VANESSA	Signature	SAOP (Email PIN)		Content Signed

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PTA 04	Data Feed Service, pta_pia_OS_Release	6/8/2026	Please define the acronyms 'HHS' and 'FOIA' on first use within the response.	
PTA 05	Data Feed Service, pta_pia_OS_Release	6/8/2026	The information detailed in the responses to questions PIA-22 and 22A will also have to be included in this response. (E.g. SSN, DUNs, Passport #, etc.)	
PTA 06	Data Feed Service, pta_pia_OS_Release	6/8/2026	Please also detail the category of individual the PII is being collected from. Please also include whether the information is being shared with another system. If it is not being shared, please indicate so.	
PTA 09	Data Feed Service, pta_pia_OS_Release	6/8/2026	Please define the acronym 'VPN' on first use within the response.	
PTA 21A	Data Feed Service, pta_pia_OS_Release	6/8/2026	Please additionally detail in this response: • Please describe, to the best of your ability, any known AI use cases. • Please include the following statement "The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks." • Please indicate if the AI tool(s) be trained using the PII collected in the system?	
PIA 26	Data Feed Service, pta_pia_OS_Release	6/8/2026	Per the privacy risk analysis checklist submitted to us, the PII will be used	

for testing purposes. Please provide a response detailing this information.

PIA 31B	Data Feed Service, pta_pia_OS_Release	6/8/2026	PIA-23 provides a contradictory response indicating that information is collected from 'members of the public'.
PIA 45	Data Feed Service, pta_pia_OS_Release	6/8/2026	Please define the acronyms 'CL', 'TLS', and 'AES' on first use within the response.
PIA 44	Data Feed Service, pta_pia_OS_Release	6/8/2026	Please also include the relevant Item # and Disposition Authority for the GRS in the response.
PTA 05	PETERS, GODISGREAT	6/16/2026	Per PIA 22, please include the following PII "Alien registration number, Employee ID Number, Criminal records, Video or Audio Identifiers or Recordings."
PTA 04	BLAND, CRYSTAL	6/17/2026	Revised your response to read "The Anata Artificial Intelligence (AI) Redaction Suite is an AI-powered document review and redaction system designed for processing government documents, particularly for Freedom of Information Act (FOIA) requests. The suite's capabilities include: 1. Identifying and redacting sensitive information such as personally identifiable information (PII), protected health information (PHI), and law-enforcement-sensitive data. 2. Using large language models (LLMs) and semantic analysis rather than relying solely on keyword matching or regular expressions. 3. Supporting FOIA exemption workflows by helping agencies determine what information should be withheld before public release. 4. Reducing the manual effort involved in reviewing large document collections. The system will support the Department of Health and Human Services (HHS) Freedom of Information Act (FOIA) office by using the AI suite to recommend potential redactions for human review. Authorized users review,

propose, edit, and finalize redactions before the system applies them to records prepared for HHS FOIA release. The AI tool(s) will not be trained using PII collected in the system. "