

General Information

PTA / PIA Name:	OS - OGC CP - QTR1 - 2026 - OS3247965	PTA / PIA ID:	4328893
Component Name:	OS - HHS OGC Casepoint	ATO Boundary Name:	HHS OGC Casepoint
Overall Status:	Complete 	# of Days - Open:	78
Submitter:		Submit Date:	3/23/2026
Next Assessment Date:	03/26/2029	Expiration Date:	3/26/2029
Office:		OpDiv:	OS
Security Categorization:	High		
Make PIA available to Public?:	No	PIA Required:	Yes
General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance	
General 02:	Is this a FISMA-Reportable system?	Yes	
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No	
General 04:	ATO Date or Planned ATO Date.	1/8/2026	
General 05:	Is the system or electronic information collection, agency or contractor operated?	Contractor	
History Log:	View History Log		

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Jon Lewin
PTA 01A:	POC Title and Organization	ISSO - OGC
PTA 01B:	POC Email Address	Jon.Lewin@hhs.gov
PTA 01C:	POC Phone Number	202-260-6156
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?	Agency

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.

Casepoint is a data discovery platform for legal, investigatory, compliance, and IT teams who struggle to get actionable insights for data-centric business processes like eDiscovery, investigations, and information requests. Casepoint empowers leading corporations and government organizations to reduce costs, lower risk, and improve time-to-insight. Casepoint's easy-to-use AI-powered platform is purpose-built for organizations that require the highest level of security and scalability to meet the evolving demands of the modern data landscape.

Casepoint Government is delivered as a Software as a Service (SaaS) offering using a multi-tenant government-only cloud computing environment and is used by government agencies to meet their complex needs, including:

Legal Holds, Regulatory Enforcement / Investigations, Litigation (eDiscovery), Freedom of Information Act (FOIA) / Public Records Request (PRR), Congressional Inquiries, Legal Data Storage, Task / Case Strategy and Management

The Casepoint Government platform includes Casepoint Legal Hold, Casepoint eDiscovery, Casepoint FOIA, Casepoint Filestore, Application Programming Interface (APIs) for cloud collections, task management, and an app builder. Casepoint Government provides agencies with the capabilities needed to manage large volumes of data in litigation, investigations, congressional inquiries, and FOIA requests, including cloud-based collections, processing, culling, review, and highly customizable productions. It also offers built-in artificial intelligence (AI) and analytics with advanced tools for predictive analysis, search, and data visualization. These AI tools are optional, customer controlled and used to assist specific, user-initiated workflows such as search, summarization, classification, and drafting to improve efficiency. All AI outputs require user review and do not take autonomous action on customer data.

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

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.	Casepoint contains the following information type and subcategories. Information and Technology Management which includes Record Retention, Information Management, Information Sharing. Law Enforcement which includes Criminal Apprehension, Criminal Investigation and Surveillance. Litigation and Judicial Activities which includes Judicial Hearings, Legal Defense, Legal Investigation, Legal Prosecution and Litigation, Resolution Facilitation, Regulatory Compliance and Enforcement, Inspections and Auditing. Within these information types and sub categories the following types of PII may be included or processed: 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., National Provider Identifier (NPI)), Financial Account Information (e.g., account numbers, credit card numbers), Device Identifiers, Name, Date of Birth, User Credentials, Mother's Maiden Name, Certificates (e.g., training certificates), Education Records, Employment Status/History, Foreign Activities, Legal Documents, Military Status/History, Email Address (Personal), Mailing Address (Personal), Phone Numbers (Personal), Email Address (Business), Mailing Address (Business), Phone Numbers (Business), Medical Records, Medical Records Number, Patient ID Number. Records maintained within the eDiscovery platform are retained for the duration of active litigation, including any period during which discovery obligations remain pending or there is a continuing need to produce documents. There is no fixed retention period applicable to all matters; retention is determined on a case-by-case basis and is driven by the specific legal, regulatory, and operational requirements associated with each matter. When data must remain available for potential future use but does not require active processing or review, it may be transitioned to near-line or dormant storage. In this state, the data remains preserved and retrievable but is not maintained in an active workspace. Once litigation is concluded, discovery obligations are fully satisfied, and there is no further legal or operational need to retain the records, the data is removed from the platform in accordance with applicable records retention schedules and disposition requirements.
PTA 05A:	Are user credentials used to access the system?	Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system.
PTA 05C:	Please identify the system that maintains the user credentials or controls access to this system.	Azure Active Directory

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.	Casepoint collects, maintains, and shares information to support HHS Office of the General Counsel's (OGC) authorized legal and administrative functions, including litigation, investigations, compliance and enforcement, and compliance with discovery and records preservation obligations. The system does not collect information directly from individuals; rather, it processes electronically stored information (ESI) obtained from HHS source systems, custodial data collections, and external parties as required by legal matters. The collection and maintenance of information is limited to what is necessary to meet legal and regulatory requirements. Information may be shared internally with authorized HHS personnel and approved contractors, and externally with courts, opposing counsel, or other authorized entities, subject to applicable legal authorities, protective orders, and confidentiality safeguards. The system does not use the information for secondary purposes unrelated to its legal and compliance mission. Categories of individuals of whom this information may apply include Federal employees, former Federal employees, contractors and subcontractors, attorneys and legal staff, individuals who are parties to, witnesses in, or otherwise referenced in legal matters handled by OGC, and members of the public whose information may appear in records subject to e-discovery. Types of PII collected vary depending on the specific litigation, investigation, compliance, or discovery obligations, but can include 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, Name, Date of Birth, User Credentials, Mother Maiden Name, Certificates (e.g., training certificates), Education Records, Employment Status/History, Foreign Activities, Legal Documents, Military Status/History, Email Address (Personal), Mailing Address (Personal), Phone Numbers (Personal), Email Address (Business), Mailing Address (Business), Phone Numbers (Business), Medical Records, Medical Records Number, Patient ID Number.
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).	platform.casepointgov.com

PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	Yes
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.	OGC Attorneys have access to upload and review e-discovery data via Single Sign On (SSO) to platform.casepointgov.com The website is publicly accessible but access is only granted by a manual process.
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.	Other technology - Does Not Collect PII
PTA 12B:	What other technology is used?	Casepoint records limited feature usage to support product improvement and does not access customer content or case data.
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?	AI is used to assist specific, user-initiated workflows such as search, summarization, classification, and drafting to improve efficiency. All AI outputs require user review and do not take autonomous action on customer data.

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

Biographical Information

Name

Date of Birth

User Credentials

Mother Maiden Name

Certificates (e.g., training certificates)

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

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.	500 – 4,999
PIA 25:	For what primary purpose is the PII used?	The e-discovery platform serves as a document processing tool that enables HHS to organize, analyze, review, redact, and produce electronically stored information (ESI) containing PII. The primary purpose of using PII within the platform is to support critical HHS functions, including conducting internal investigations, responding to litigation discovery requests, complying with subpoenas, and fulfilling other legal and regulatory obligations such as Freedom of Information Act (FOIA) and Privacy Act (PA) requests, Government Accountability Office (GAO) inquiries, and Congressional requests.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	HHS makes no secondary use of the PII.
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.	While the system doesn't solicit the SSN directly, It does maintain legal and financial documents that contain the SSN.
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.	E.O. 9397

PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	The legal authority for maintaining this system derives from various statutes, regulations, rules, and orders pertaining to the subject matter of litigation, administrative complaints, or adverse personnel actions, including but not limited to the Public Health Service Act, Social Security Act, Civil Rights Act, and Federal Food, Drug and Cosmetic Act. Additionally, the system collects PII in accordance with federal laws and guidance such as the Federal Rules of Civil Procedure, Federal Rules of Criminal Procedure, and Congressional and Committee Procedures codified at 2 U.S.C. Chapter 6. The specific legal authority governing the original collection of data and the applicable System of Records Notice (SORN) are determined by the context of the data being analyzed. Records related to litigation discovery are generally covered by the Office of the General Counsel Litigation Files, Administrative Complaints and Adverse Personnel Actions SORN, published at 47 FR 45514, 45542 (October 13, 1982), and updated at 59 FR 55845 (November 9, 1994) and 83 FR 6591 (February 14, 2018). Furthermore, 5 U.S.C. § 301 provides authority for the establishment of systems and processes necessary to maintain records and conduct agency activities.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA 29A:	Please specify which PII data elements are used to retrieve records.	Records in the system are typically retrieved by one or more PII data elements, most commonly custodian name. Depending on the specific requirements of a matter, litigation, or investigation, litigators, FOIA analysts, and other authorized users may retrieve records using various PII elements to identify relevant responsive information.
PIA 29B:	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.	Office of the General Counsel Litigation Files, Administrative Complaints and Adverse Personnel Actions SORN, published at 47 FR 45514, 45542 (October 13, 1982), and updated at 59 FR 55845 (November 9, 1994) and 83 FR 6591 (February 14, 2018).
PIA 30:	Identify the sources of PII in the system.	Government Sources Within the OPDIV Other HHS OPDIV
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.	No. The system is used within the organization and, generally, does not involve collection from directly from the public. Data collection for the system occurs within the agency and does not involve collection of data from more than 10 members of the public.

PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	Yes
PIA 32A:	Identify with whom the PII is shared or disclosed.	Other Federal Agency/Agencies Private Sector
PIA 32B:	For each disclosure, name the organizations/systems the system shares PII with and the purpose(s) of the disclosure.	Other Federal Agencies (Department of Justice (DOJ), equities partners); Private Entities (litigation and FOIA productions); Congress (oversight productions). HHS OGC may produce and share data from the system with various entities as authorized or required by law, including courts, opposing counsel, defendants, law enforcement agencies, litigation partners, vendors, and other organizations or individuals. When HHS OGC shares information with external entities, it does so under specific legal frameworks and protections. Disclosures typically occur pursuant to court-approved protective orders, in response to FOIA/PRR requests with appropriate exemptions or exceptions applied, to the Department of Justice serving as agency counsel, or in response to Congressional requests with appropriate assertions of privilege. Disclosures are made in accordance with applicable legal requirements and the purposes of the underlying matter, litigation, or investigation.
PIA 32C:	List any agreements in place that authorize the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	None
PIA 32D:	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.	Casepoint logs and tracks access to the system and data productions.
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.

The e-discovery platform serves as a repository for information gathered from other HHS record systems and third-party sources for litigation and e-discovery purposes. Due to the nature of these collections, providing direct notice and obtaining consent from individuals before processing their information is often impractical.

HHS employees and system users receive notice through warning banners indicating that information transmitted through HHS systems may be monitored, intercepted, searched, and/or seized by the department, and that users have no reasonable expectation of privacy in such information.

Where feasible, HHS provides notice and consent options at the original point of collection. When the e-discovery platform imports PII from other HHS systems, individuals receive notice through the Privacy Act Statements, SORNs, and PIAs associated with those source systems, which explain available choices regarding collection, use, and disclosure of PII. When the platform receives data from third parties, such as healthcare providers, health plans, or government agencies, HHS cannot provide advance notice, and the originating entity is responsible for providing required notices to individuals.

For information collected pursuant to HHS requests, notice is included in the request itself (e.g., in letters or compulsory process documentation). Litigants are informed that courts may require HHS to search for and produce relevant agency records during litigation. When HHS collects information through discovery, court orders, or investigations, individual notice may not be provided, as collection, use, and disclosure are governed by federal law, discovery rules, and court orders.

This PIA serves as public notice of HHS's collection and use of information in the e-discovery platform. When direct notice is impractical or not legally required, HHS provides constructive notice through its Privacy Policy and PIAs.

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.

This system receives information from other systems and that system is responsible for notifying and obtaining consent from individuals whose PII is in the system. Through evaluation and review of PIAs and SORNs, HHS ensures that notices are revised to reflect changes in practices or policies that may impact Privacy. The HHS OGC SORN provides notice of relevant changes in HHS OGC system of records at 47 FR 45514, at 45542 (10/13/82); updated 59 FR 55845 (11/9/94), 83 FR 6591 (2/14/18), <https://www.govinfo.gov/content/pkg/FR-1982-10-13/pdf/FR-1982-10-13.pdf>.

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.	The HHS Privacy Act webpage, https://www.hhs.gov/foia/privacy/index.html , provides individuals with guidance and information on addressing Privacy Act concerns. Inquiries, complaints, and requests are handled on a case-by-case basis.
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.	HHS reviews information collected during investigations, enforcement actions, and other mission-critical activities to ensure it is accurate, complete, and timely as required by the specific activity. When applicable, HHS staff conduct research to verify the accuracy and completeness of obtained information and/or require individuals submitting information to certify its accuracy (e.g., witness statements or documentation in legal proceedings). However, the e-discovery platform typically does not collect personal information directly from individuals. Instead, it receives copies of records obtained from other HHS recordkeeping systems and third-party sources. Therefore, HHS relies on the originating HHS program or external entity that initially collected the information to ensure the accuracy and completeness of PII. Additionally, HHS does not use the e-discovery platform as an authoritative source for PII about individuals, nor does it use the platform to alter PII in the original records. Any inaccurate or incomplete information, when identified, would be corrected in the source systems. Information incorporated into the e-discovery platform is subject to appropriate security and chain-of-custody controls to protect sensitive information, including PII, from compromise, loss, or alteration, and to ensure the integrity of evidentiary materials from the point of incorporation into the platform. The e-discovery platform maintains comprehensive logging capabilities to track data modifications and provide usable audit trails, ensuring ongoing data integrity and accountability.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators Contractors
PIA 38A:	Select the type of contractor.	HHS/OpDiv Direct Contractors Third-Party Contractor (Contractors other than HHS 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.	HHS Office of General counsel users require access to the system to review, analyze, and prepare data in the system to respond to litigation discovery, congressional requests, FOIA requests, and internal investigations. Administrators require access to the system to provide support and maintenance of the system. HHS OGC also contracts with direct and third-party contractor vendors to obtain legal support services and products for electronically processing, hosting, storing, and reviewing information related to HHS investigations, litigation, and oversight activities. Further, HHS contractors, including contractors providing legal support services and outside counsel who have executed legal services agreements with HHS to provide support for litigation, may have access to the system.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Users of the e-discovery platform are granted access to roles set within the platform. Internal and external users of the platform must have approval of the supervisory attorney managing the litigation, investigation, or oversight response and the contracting officer representative.
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 granted on a need-to-know basis and roles are limited to a users' specific function and needs, regulating a user's ability to update data or access information or data beyond that needed to perform the necessary duties. Access is only granted to the workspace that applies to the user therefore separating out data from unrelated cases for specific users. A user's access is also tracked by the e-discovery platform.
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 users must complete computer security awareness training annually, as well as review and agree to comply with HHS information technology Rules of Behavior both prior to access the HHS network and annually thereafter. System administrators must complete additional professional training, which includes security training.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	Training on Casepoint itself is provided by them as needed

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).	National Archives and Records Administration (NARA) approved Records Retention Schedule DAA-0468-2012-0016 addresses records related to subpoenas for testimony, subpoenas duces tecum, or other formal testimony or document production requests in litigation in which HHS is not a party and includes the agency's document production. The agency's document production and case files are temporary and destroyed 3 years after cutoff. NARA approved Records Retention Schedule DAA-0468-2012-0009-0018 addresses litigation case files, including correspondence, decisions, and similar documents. Case files with no precedential value are destroyed 2 years after cut off. Case files with precedential value are transferred to the Federal Records Center (FRC) two years after cutoff and destroyed 20 years after cutoff. And NARA General Schedule DAA-GRS-2016-0002-0001 addresses case files created in response to FOIA requests. Records are destroyed 6 years after final agency action or 3 years after final adjudication by the courts. Copies of requested or produced records are subject to the aforementioned retention periods. Record copies of requested records remain covered by their original disposal authority.
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 safeguards include user training; system documentation that advises on proper use; implementation of need-to-know and minimum necessary principles when awarding access, and others. Technical safeguards include use of single-sign-on or multi-factor access authentication, firewalls, network monitoring, and lapsed account safeguards. For physical controls, Casepoint is hosted on the Microsoft Azure and Casepoint private cloud, and Azure's FedRAMP authorization inherently includes physical security measures (e.g., data center access restrictions).

Review and Comments			
OpDiv Privacy Analyst Review			
Privacy Analyst Review Decision:	Approved	Privacy Analyst Review Date:	3/23/2026
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:	3/23/2026
SOP Review Comments:		# of Days - SOP Review:	0

Agency Privacy Analyst Review			
Agency Privacy Analyst Review Decision:	Approved	Agency Privacy Analyst Review Date:	3/24/2026
Agency Privacy Analyst Review Comments:	Reviewer: Christopher Akhibi 3/24/2026 AI review completed. This PIA is ready for SAOP review and approval. 3/20/2026 Please see comments and update accordingly: PTA 5C: Please, change Azure 'ID' to Azure 'AD' Azure Active Directory PIA 44: Please, spell out acronym 'FRC' first time use Federal Records Center.	# of Days - APA Review:	1

SAOP Review					
SAOP Review Decision:		Approved	SAOP Review Date:		3/27/2026
SAOP Review Comments:			# of Days - SAOP Review:		3
SAOP Signature					
Date	User	Type	Name	Original Value	New Value
3/27/2026 1:37 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 08A	Data Feed Service, pta_pia_OS_Release	2/6/2026	platform.casepointgov.com	
PTA 08B	Data Feed Service, pta_pia_OS_Release	2/12/2026	The website itself is accessible on non govt computers but logins are restricted to manually designated accounts	
PTA 04	Data Feed Service, pta_pia_OS_Release	2/26/2026	1 - Please remove the bullet points from this response as they are not 508 compliant. Please reformat the information into a list or space with carriage returns. 2 - Please define the following acronyms on first use within the response: SaaS, FOIA, PRR, and APIs. 3 - As the system is using AI, within this response: • Please describe, to the best of your ability, any known uses cases for the AI. • Please include the following statement in the response "The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks." • Please detail if the AI tool be trained using the PII collected in the system?	
PTA 05	Data Feed Service, pta_pia_OS_Release	2/26/2026	1 - Please remove the bullet points from this response as they are not 508 compliant. Please reformat the information into a list or space with carriage returns. 2 - Please detail the length of time the information will be stored in the response. 3 - The types of information listed in this response should align with the information listed in PTA-06 and PIA-22. Please update the response accordingly.	
PTA 09	Data Feed Service, pta_pia_OS_Release	2/26/2026	Please define the acronym 'SSO' on first use within the response.	

PTA 20A	Data Feed Service, pta_pia_OS_Release	2/26/2026	Can you please detail which third party application or websites are being used with the system? If none are being used currently and the system only supports their potential integration, please update the response for question 20 to a 'no'.	
PIA 32B	Data Feed Service, pta_pia_OS_Release	2/26/2026	Please define the acronym 'DOJ' on first use within the response.	
PTA 04	AKHIBI, CHRISTOPHER	3/10/2026	Please, spell out SaaS first time use in the following sentence. Casepoint Government is delivered as a SaaS "Software as a Service (SaaS)"	
PTA 06	AKHIBI, CHRISTOPHER	3/10/2026	Please, spell out "OGC" first time use of the acronyms.	
PTA 05	AKHIBI, CHRISTOPHER	3/10/2026	Please, spell out: National Provider Identifier (NPI) Use Mother's Maiden name instead <u>Mother</u> Maiden Name	
PTA 05C	AKHIBI, CHRISTOPHER	3/20/2026	Please, confirm and correct the follow Azure ' ID ' Azure ' AD ' Azure Active Directory	
PIA 44	AKHIBI, CHRISTOPHER	3/20/2026	Please, spell out acronym ' FRC ' first time use Federal Records Center.	
PTA 21	BLAND, CRYSTAL	3/24/2026	3/24/2024 AI Review is completed and Cleared.	OS3247965 EMAIL_RE AI Review.msg