Privacy Impact Assessment (PIA)

CASEPOINT

March 2026
Date

System/Collection Overview
Casepoint is a cloud-based Software as a Service (SaaS) platform designed to support the Agency's e-discovery process by collecting, managing, and preserving electronically stored information. It offers comprehensive capabilities, including data collection and processing, advanced analytics, document review, and data production. Additionally, the system facilitates legal hold notifications and provides tools for managing Freedom of Information Act (FOIA) requests. This system is essential to the Agency's operations, providing critical capabilities for addressing legal, regulatory, and investigative requests. It supports the Agency's compliance with the Federal Rules of Civil Procedure (FRCP) and supports the Agency in responding to entities such as the Federal Housing Finance Agency (FHFA) Office of Inspector General (OIG), Congress, and the Government Accountability Office (GAO).

Section 1.0 Characterization of the Information

The following questions address the scope of the personally identifiable information (PII) requested and/or collected. PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. PII includes, but is not limited to, name, address, Social Security number, date of birth, financial information, and demographic information.

#	Question and Response
1.1	***What and whose PII is being collected, used, disseminated, or maintained?***
	The system collects electronically stored information relevant to litigation, investigations, FOIA/Privacy Act requests, or other legal proceedings. The information collected originates in other FHFA systems, including the Microsoft365 suite of products, email archives, the Agency's shared electronic filing system (IMS), and other FHFA file systems. The data collected includes, but is not limited to, emails, messages, documents, and databases. The system also maintains a list of users, including names and email addresses. Due to the nature and purpose of the system, the scope of PII collected is broad and could include any PII within the Agency's information technology network. The system may collect and store PII, including, but not limited to, address (home or business), email address (personal or business), date of birth, Social Security number (SSN), driver's license number, passport number, biometric identifiers (e.g., fingerprints, photographs), demographic information (e.g., sex, race, religion), medical information, education records, financial information (including salary and benefits information), military records, and bankruptcy or criminal records. The system does not collect PII directly from users. The information includes the PII of FHFA employees and contractors, members of the public,

	and employees of entities that FHFA regulates.
1.2	***If Social Security Numbers (SSNs) are included, describe in detail:*** ***1) The business justification for collecting or using SSNs;*** ***2) The consequences if SSNs are not collected or used;*** ***3) How the SSNs will be protected while in use, in transit and in storage.***
	SSNs, in whole or in part, are not specifically collected and stored by the system but may be collected by and maintained in the system if contained in documents that are responsive to an eDiscovery request. FHFA cannot preemptively exclude SSNs from its eDiscovery process as they may be contained in documents responsive to eDiscovery requests or otherwise relevant to pending litigation and therefore are necessary to meet the Agency's legal obligations. SSNs are protected as described in Section 6.
1.3	***How is the PII obtained? If individuals are not providing their own PII directly, describe where the information originates and any intermediaries it goes through before being provided to FHFA. Include a description of the mechanism by which the PII is provided to/obtained by FHFA.***
	The system collects information directly from existing data sources, including, but not limited to, Microsoft 365, email archives, the Agency's shared electronic filing system, and other FHFA file systems or databases. The information is copied from the data source and uploaded to the system, or the system ingests the files and metadata by directly connecting to the data sources.
1.4	***How will the PII be used and for what purpose?***
	The information stored in the system is used to support the Agency's eDiscovery program and to facilitate the management of document production in response to litigation, investigations, FOIA/Privacy Act requests, or other legal matters. Information collected may also be used to address inquiries from Congress, the Office of Inspector General, or the Government Accountability Office.
1.5	***Is there a risk that PII other than that described above will be collected? If no, explain why not. If yes, explain the risk and how the risk is mitigated.***

	No, information uploaded or directly ingested into the system is limited to that which has been identified as being potentially responsive to an eDiscovery request. Such requests generally use search terms, date ranges, and custodian names to identify potentially responsive documents. While PII that is not responsive may be collected, the PII collected by the system is accessible only to those personnel with a business need to access and review the information. Further, processes exist to review the PII collected and redact or withhold information from production if legally appropriate.
1.6	***Is there a risk that the PII collected will be inaccurate? If no, explain why not. If yes, explain the risk and how the risk is mitigated.***
	Yes, there is a risk that information collected as part of the eDiscovery process could be inaccurate. Data collection may include outdated, incomplete, or erroneous records without context. The Agency implements a review process to verify the relevance of the collected data, however any process to correct inaccurate information would be addressed at the system-level and not as part of the eDiscovery process, which must take into account the need to preserve potential evidence in its original state.

Section 2.0 General

The following questions address general information about the information in the system, including how the information will be used and for what purpose.

#	Question and Response
2.1	***What is the legal authority for the collection?***
	5 U.S.C. § 552 (Freedom of Information Act); 5 U.S.C. § 552a (The Privacy Act of 1974); Federal Rules of Civil Procedure; 31 U.S.C. § 712 (GAO access authority).
2.2	***Is the collection of information subject to the Paperwork Reduction Act? If yes, what is the OMB Control Number for the collection?***
	There is no collection of information subject to the PRA.
2.3	***Is this a new PIA or an update to an existing PIA?***

	This is a new PIA.
2.4	***Is the system internally operated or operated by a third-party (e.g., contractor)? If not internally operated, please identify the third party.***
	The system is operated by a third-party contractor, Casepoint.
2.5	***How is the risk of improper use of the PII by FHFA employees/contractors mitigated? If PII is shared with third parties, how will the risk of improper use by those parties be mitigated?***
	The system is only accessible by approved staff. Access is granted on an as-needed basis and limited to individuals directly involved in the legal matter. The risk of improper use of the information is further mitigated by providing training to FHFA employees/contractors and by regularly notifying them of adverse consequences for improper use of FHFA information. The risk of misuse by third parties is mitigated by communicating to third-party recipients any relevant restrictions on the sharing and/or use of the information. PII produced in litigation may also be subject to protective orders where appropriate.

Section 3.0 Retention

The following questions address how long PII will be retained after the initial collection.

#	Question and Response
3.1	***How long is the PII retained?***
	The system temporarily stores information. Once the information has been reviewed and prepared for production or dissemination (including redacting information, where appropriate) a document production is prepared and the information is removed from the system. As such, documents in the system are temporary and destroyed upon creation or update of the final record, or when no longer needed for business use, whichever is later.
3.2	***Has a retention schedule been approved by FHFA's Records Management Office and National Archives and Records Administration (NARA)? If yes, provide the corresponding General Record Schedule (GRS) or FHFA specific Records Schedule number.***

	GRS 5.2.020 Intermediary records.

Section 4.0 Notice, Individual Access, and Correction

The following questions address notice to the individual, the individual's right to consent to uses of the PII, the individual's right to decline to provide PII, and the individual's ability to ensure the accuracy of the PII collected about them.

#	Question and Response
4.1	***Is information about an individual retrieved by an individual's name or personal identifier such as name, email address, or date of birth? If yes, identify the applicable System of Record Notice (SORN).***
	No, the system is a temporary repository of data. No searches for information about an individual are conducted using that individual's name or personal identifier and accordingly, this system is not a system of records.
4.2	***How is notice about the collection of PII provided to an individual prior to collection from that individual? If notice is not provided, explain why.***
	Not applicable (NA). Information is collected from data sources within the Agency, not directly from an individual.
4.3	***Is an individual's response to the request for PII voluntary or mandatory?***
	NA. Information is collected from sources within the Agency, not directly from an individual.
4.4	***What are the consequences if an individual declines to provide the requested PII?***
	NA. Information is collected from sources within the Agency, not directly from an individual.

4.5	***What are the procedures that allow individuals to gain access to their PII?***
	NA. The system is not a system of records as defined under the Privacy Act. Individuals may make Privacy Act requests for records contained in the underlying systems of records to the extent those systems are subject to the Privacy Act.
4.6	***What are the procedures for individuals to correct or update information about them?***
	NA. The system is not a system of records as defined under the Privacy Act. Individuals may make record correction requests with respect to records that are contained in an underlying system that is subject to the Privacy Act.

Section 5.0 Sharing and Disclosure

The following questions address the content, scope, and authority for sharing PII.

#	Question and Response
5.1	***Is PII shared with other offices or divisions within FHFA? If yes, identify the other offices/divisions and describe the purpose of or business need for sharing the PII.***
	PII is shared within the Office of General Counsel (OGC) with individuals who have a business need to access the information, including attorneys, litigation support staff, and other staff and attorneys supporting FOIA and Privacy Act requests. PII may also be shared with individuals in other offices when necessary to respond to an information request. Staff from the Office of the Chief Information Officer may also access data as part of system maintenance.
5.2	***Is PII shared with individuals or entities outside of FHFA? External entities include other Federal agencies, state or local governments, regulated entities, FHFA-OIG, and Congress. External entities do not include FHFA contractors that receive PII as needed in their performance of work for FHFA.*** ***If yes, please identify the PII shared, and for what purpose or business need.***

	PII that is responsive to an information request from non-FHFA parties or other entities is shared with the requester to the extent consistent with applicable law. Requestors may include Congress, FHFA-OIG, FOIA/Privacy Act requestors, or opposing parties in litigation.
5.3	***If PII is shared with external entities, describe how the information sharing is compatible with the purpose for which the PII was collected.*** • ***If a SORN applies, identify the applicable routine uses in the SORN listed in Section 4.1.*** • ***If a SORN does not apply, describe 1) whether notice of the PII sharing was provided and if so, how; and 2) how the sharing of PII is consistent with the purpose for which the information was collected. Sharing with Congress, FHFA-OIG or the Government Accountability Office pursuant to the statutory authorities of those entities need not be addressed.***
	Due to the nature of the eDiscovery process, PII that is provided to external parties may potentially be obtained from any one or more of FHFA's systems of records that are described in a SORN and applicable to the underlying source of the records in Casepoint. FHFA's SORNs are available at: FHFA Privacy Act Systems of Records Notices (SORN) | FHFA. Any information shared shall be in accordance with the routine uses listed in the applicable SORNs.
5.4	***Describe how the risk of intentional or inadvertent disclosure of PII by FHFA employees/contractors is mitigated. (Address both disclosures within FHFA and disclosures to external parties.)***
	Access is restricted to authorized personnel through role-based access, ensuring employees and contractors only access the minimum data necessary for their duties. The risk of improper disclosure is further mitigated by providing training, including role-based privacy training, to FHFA employees/contractors with respect to protecting PII. Documents are also marked as Controlled Unclassified Information, where appropriate.
5.5	***If PII will be shared with external parties, describe how the risk of improper disclosure of the information by individuals or entities outside of FHFA is mitigated.***

	When PII is shared with external parties the risk of improper disclosure may be mitigated through the use of confidentiality agreements and protective orders that strictly limit the use of the information to the specific legal matter. Information may also be transmitted using secure transfer protocols and Agency-approved portals. Sensitive information is labelled and redacted as appropriate, and recipients are advised of any restrictions on the sharing and/or use of the information.

Section 6.0 Technical Access and Security

The following questions address technical safeguards and security measures.

#	Question and Response
6.1	***Will individuals other than FHFA employees and FHFA contractor personnel performing official FHFA duties have access to the system containing the PII? If yes, how will access to the system be granted and controlled with respect to these external parties?***
	No.
6.2	***Is any system-specific training or guidance related to PII or privacy provided to users of the system? If so, please describe.***
	No, system-specific training is not provided.
6.3	***Describe the technical/administrative safeguards in place to protect the PII.*** Casepoint data is encrypted in transit and at rest. The Casepoint private cloud storage devices are FIPS enabled, encrypting all data at rest using Azure Storage Service Encryption. This service leverages Azure Key Vault for creating, using, and storing encryption keys, which are further protected by a FIPS-validated hardware security module (HSM). All SQL server connections are mandated to use TLS 1.2 with AES-256 encryption as specified in the connection string.
	Casepoint obtained their FedRAMP Authorization on April 1, 2025. As part of the FHFA continuous monitoring process, an annual review of a subset of the system's security controls is performed. FHFA has developed a system security and privacy plan that describes the Agency's implementation of controls that are the responsibility of FHFA as the Customer Agency. This includes the implementation of single sign-on authentication, procedures for securely managing access to the system, assigning permissions based on the concept of least privilege, and generating and reviewing audit logs.