



Privacy Impact Assessment (PIA)

SOFTLINX REPLIFAX

(Name of the Information System or Information Collection)

April 2026

Date

System/Collection Overview

Softlinx Replifax is a secure, electronic faxing solution used to transmit and receive fax communications through an encrypted cloud-based interface. It enables FHFA employees and contractors to send and receive faxes electronically using their Outlook email accounts. Fax images are securely stored in the Softlinx Replifax cloud environment, and authorized FHFA administrators can access or retrieve them through the Replifax web console for auditing or troubleshooting purposes. Fax images may contain a range of personally identifiable information (PII) types. Faxes received through Softlinx are often human resources (HR) documents that can contain a variety of PII including contact information, financial information, and demographic information.

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	<p><i>What and whose PII is being collected, used, disseminated, or maintained?</i></p> <p>Information in the system may contain an individual's name, business email address, date of birth, business phone number, sex, ethnicity, as well as various types of PII from HR documents that could include other business and personal contact information, financial information, demographic information, Social Security number, service history, salary information, information from medical documents and information from court documents. The individuals whose information is collected in the system are FHFA and other federal agency employees and contractors.</p>
1.2	<p><i>If Social Security Numbers (SSNs) are included, describe in detail:</i></p> <ol style="list-style-type: none"><i>1) The business justification for collecting or using SSNs;</i><i>2) The consequences if SSNs are not collected or used;</i><i>3) How the SSNs will be protected while in use, in transit and in storage.</i>

	<p>SSNs are collected in the system if they are included in the documents being sent to FHFA through the system. The specific business justification for sending SSNs depends on the purpose for which the document is being sent, but it is generally related to performing HR functions. FHFA employees and contractors do not send full SSNs through the system, however SSNs are received from third parties through Softlinx. All outgoing documents with SSNs are either redacted to only show the last four digits or removed completely. All outgoing faxes through the system are protected by Zix email encryption software.</p>
1.3	<p><i>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.</i></p>
	<p>PII uploaded to the system is contained in existing documents and therefore the system does not serve as the point of collection. PII may be provided directly by individuals or from other sources through HR-related processes.</p>
1.4	<p><i>How will the PII be used and for what purpose?</i></p>
	<p>The system is generally used to send and receive PII to perform HR-related functions.</p>
1.5	<p><i>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.</i></p>
	<p>No. As noted in Section 1.1, the scope of PII that may be stored or processed by the system is very broad and covers any type of PII that might be relevant to HR functions.</p>
1.6	<p><i>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.</i></p>

There is a risk that PII in documents sent through the system is inaccurate. However, these errors are unrelated to the system itself and are addressed via separate business processes.

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	<p><i>What is the legal authority for the collection?</i></p> <hr/> <p>12 U.S.S 4513(a)(2)(B).</p>
2.2	<p><i>Is the collection of information subject to the Paperwork Reduction Act? If yes, what is the OMB Control Number for the collection?</i></p> <hr/> <p>The collection of information is not subject to the Paperwork Reduction Act.</p>
2.3	<p><i>Is this a new PIA or an update to an existing PIA?</i></p> <hr/> <p>This is a new PIA.</p>
2.4	<p><i>Is the system internally operated or operated by a third-party (e.g., contractor)? If not internally operated, please identify the third party.</i></p> <hr/> <p>The system is hosted and operated by a third-party vendor, Softlinx.</p>

	<i>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?</i>
2.5	The risk of the improper use of PII by FHFA employees and contractors is mitigated in several ways. New system users receive a user guide and hands-on training to instruct them on how to use the system and the proper handling of transmitted information. Further, FHFA employees and contractors receive annual and role-based privacy training to maintain their awareness of proper use of PII and annually complete FHFA's Rules of Behavior, which notify them of the consequences of misuse of PII. Documents sent to third parties are also marked as Controlled Unclassified Information, 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	<p><i>How long is the PII retained?</i></p> <p>Fax files are deleted from the system once the default 30-day retention period is over.</p>
3.2	<p><i>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.</i></p> <p>GRS 5.2, item 020 (Intermediary Records).</p>

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	<p data-bbox="232 443 1458 510"><i>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).</i></p> <p data-bbox="232 646 277 674">No.</p>
4.2	<p data-bbox="232 795 1373 863"><i>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.</i></p> <p data-bbox="232 949 1443 1016">This is not applicable. The PII is contained in existing documents and therefore is not collected directly from individuals for the purposes of this system.</p>
4.3	<p data-bbox="232 1152 1123 1180"><i>Is an individual's response to the request for PII voluntary or mandatory?</i></p> <p data-bbox="232 1287 1443 1354">This is not applicable. The PII is contained in existing documents and therefore is not collected directly from individuals for the purposes of this system.</p>
4.4	<p data-bbox="232 1488 1214 1516"><i>What are the consequences if an individual declines to provide the requested PII?</i></p> <p data-bbox="232 1623 1443 1690">This is not applicable. The PII is contained in existing documents and therefore is not collected directly from individuals for the purposes of this system.</p>

4.5	<p><i>What are the procedures that allow individuals to gain access to their PII?</i></p>
	<p>Not applicable. This system contains PII from existing documents. To the extent those documents are contained in a system of records subject to the Privacy Act, individuals may make Privacy Act requests with respect to those systems. Individuals may submit a Privacy Act request to FHFA's Privacy Act Officer pursuant to 12 CFR §1204.3(b). More information is available at FHFA's Privacy webpage: https://www.fhfa.gov/about/privacy.</p>
4.6	<p><i>What are the procedures for individuals to correct or update information about them?</i></p>
	<p>Not applicable. The system contains PII from existing documents. To the extent those documents are contained in a system of records subject to the Privacy Act, individuals may make amendment requests under the Privacy Act with respect to those systems. Individuals may submit a request to amend or correct records to FHFA's Privacy Act Officer pursuant to 12 CFR § 1204.3(d). More information is available at FHFA's Privacy webpage: https://www.fhfa.gov/about/privacy.</p>

Section 5.0 Sharing and Disclosure

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

#	Question and Response
5.1	<p><i>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.</i></p> <p>Within FHFA, information is shared with a variety of systems including HR and security systems, depending on the business function it was being sent for. The documents would be received from outside of FHFA, and then manually downloaded and sent to whatever office or system, primarily HR systems, it needs to be sent to in order to perform the business function.</p>
5.2	<p><i>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.</i></p>

	<p>Documents, and the information contained therein, are sent through the system to external entities to fulfill various business functions. These external entities could be Federal agencies, courts, law enforcement agencies, etc., depending on the business function that is being fulfilled. The PII shared could be any of the data elements mentioned in question 1.1.</p>
5.3	<p><i>If PII is shared with external entities, describe how the information sharing is compatible with the purpose for which the PII was collected.</i></p> <ul style="list-style-type: none"> • <i>If a SORN applies, identify the applicable routine uses in the SORN listed in Section 4.1.</i> • <i>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.</i> <p>Various SORNs, including FHFA-10, Employee Benefits Records and FHFA-15, Payroll, Retirement, Time and Attendance, and Leave Records, may be applicable depending on the source of the information being transmitted. FHFA’s SORNs are available at: https://www.fhfa.gov/about/privacy/systems-of-records-notices. Any sharing of PII outside of FHFA is required by Agency policy to comply with routine uses identified in the applicable SORN. As the system only contains PII in existing documents, notice regarding the sharing would be provided outside of the system during the initial collection.</p>
5.4	<p><i>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.)</i></p> <p>The risk of intentional or inadvertent disclosure of PII by FHFA employees and contractors is mitigated by system users verifying that outgoing faxes were sent to the correct recipient by receiving and reviewing the confirmation of receipt notice from the system. The information is also encrypted in transit and is sent directly to the intended recipients’ email accounts.</p>
5.5	<p><i>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.</i></p>

	<p>The risk of improper disclosure of the information by individuals or entities outside of FHFA is mitigated by notifying the recipients of the information's status as PII through document markings and other communications, where appropriate. Since recipients are generally individuals who regularly work with PII (e.g., other federal HR departments), recipients will generally also have procedures in place to appropriately protect PII.</p>
--	--

Section 6.0 Technical Access and Security

The following questions address technical safeguards and security measures.

#	Question and Response
6.1	<p><i>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?</i></p> <p>No individuals other than FHFA employees and contractor personnel have access to the FHFA PII contained in the system.</p>
6.2	<p><i>Is any system-specific training or guidance related to PII or privacy provided to users of the system? If so, please describe.</i></p> <p>The FHFA Help Desk provides a user guide to each new Softlinx Replifax user and conducts hands-on training by assisting with sending and receiving test faxes when assigning a new fax number. This ensures that users understand system functionality, secure faxing procedures, and proper handling of transmitted information.</p>
6.3	<p><i>Describe the technical/administrative safeguards in place to protect the PII.</i></p> <p>When sending a fax through the system, a cover letter is used that includes a Controlled Unclassified Information notice. The faxes are also secured using Zix encryption software, which provides encryption in-transit.</p> <p>Data at rest is encrypted using AES-256 encryption, and transmitted using TLS v1.2 for web, and v1.3 for email to fax transmission.</p>