Privacy Impact Assessment (PIA) Template

OFFICE OF HUMAN RESOURCES (OHRM) EMERGENCY CONTACT LIST

September 2023

Tasha L. Cooper
Senior Agency Official for Privacy
(202) 649-3091
Tasha.Cooper@FHFA.gov

System Owner(s)			
Name	**E-mail**	**Division/Office**	**Office or Mobile Phone Number**
Rosalyn Moultrie-Matthews	rosalyn.moultrie-matthews@fhfa.gov	OHRM	202-649-3754
Executive Sponsor			
Name	**E-mail**	**Division/Office**	**Office or Mobile Phone Number**
Tami B. Smith	tami.smith@fhfa.gov	OHRM	202-649-3444
System Overview			
The OHRM Emergency Contact List is a Microsoft Excel spreadsheet that will be utilized to notify designated emergency contacts of OHRM employees in the event of an emergency. The spreadsheet will be maintained on the M:// Drive and will be restricted to individuals with a business need to know.			

Section 1.0 Characterization of the Information

The following questions define the scope of the information requested and/or collected as well as reasons for its collection as part of the System/Collection being procured or developed. The questions address all information collected, with more emphasis provided on the collection of PII, such as name, address, social security number, date of birth, financial information, etc.

#	Question	Response
1.1	What information types (e.g., name, date of birth, business contact information, demographic) is being collected, used, disseminated, or maintained in the System/Collection?	This collection includes personal contact information, which includes but is not limited to the individual Office of Human Resource Management (OHRM) employee's name, personal email address, personal phone number, and business phone number, as well as name and phone number of the individual identified as the OHRM employee's emergency contact.
1.2	What or who are the sources of the information provided to FHFA and included in the System/Collection?	The source of the information being collected is each individual OHRM employee.
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	The purpose of this collection is to identify an individual for OHRM officials to contact in the event of a medical or other emergency involving the OHRM employee during official duty time, while engaged in work related activities/events or on-site at FHFA headquarters.
1.4	How is the information provided to or otherwise obtained by FHFA?	Information will be collected by the OHRM Office Manager by email. The OHRM Office Manager will add collected information to a spreadsheet that will be saved on the M Drive. Access to the spreadsheet will be limited to the OHRM executive team and the OHRM Office Manager.

#	Question	Response
1.5	Are Social Security Numbers (SSN) being collected or used in the System? • If yes: 1) Describe in detail 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. • If no, state "N/A" in the response section.	N/A, social security numbers will not be collected.

Section 2.0 Uses of the Information

The following questions delineate the use of information and the accuracy of the data being used.

#	Question	Response
2.1	How will the information be used and for what purpose?	The information will be used to notify the OHRM employee's emergency contact should an emergency of medical or other nature occur to the employee while the employee is on-site at FHFA headquarters.
2.2	Describe any types of measures or processes in place to ensure that information is only used in the manner for which it was collected.	Access to the information will be limited to the OHRM executive team and the OHRM office manager. Information will be used only in the case of an emergency directly involving the injured OHRM employee.

Section 3.0 Retention

The following questions outline how long information will be retained after the initial collection.

#	Question	Response
3.1	How long is the information retained?	Information is retained as long as the employee is employed within OHRM.
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.	Yes. The records are covered by 6.2 – Routine Office Administration – Destroy or delete 3 years after cut-off.

Section 4.0 Notice, Access, Redress and Correction

The following questions are directed at notice to the individual, the individual's right to consent to uses of the information, the individual's right to decline to provide information, and an individual's ability to ensure the accuracy of the information collected about them.

#	Question	Response

#	Question	Response
4.1	Is the information in this System/Collection retrieved by an individual's name or personal identifier such as an SSN or other identification? • If no, please put "no" in the Response section. • If yes, the System/Collection will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)). Please provide the SORN(s) name and number or indicate that a SORN is in progress.	Records are retrieved by the name of the individual on whom they are maintained. This collection of information is covered by FHFA-14: Emergency Notification System.
4.2	How is notice about the collection of PII provided to individuals prior to the collection for the System/Collection (e.g., direct notice, Privacy Act Statement or public notice, SORN)? • If notice is not provided, explain why not. • If notice is provided, please provide a screenshot or PDF of the notice statement.	An email requesting the provision of emergency contact information that contains a Privacy Act Statement will be provided to OHRM employees.
4.3	Is an individual's response to the request for information voluntary or mandatory?	Voluntary.
4.4	What are the consequences if an individual declines to provide the information?	Failing to provide an emergency contact can result in the Agency's inability to notify the relevant person(s) of a medical or similar emergency involving the OHRM employee.
4.5	What are the procedures that allow individuals to gain access to their information?	OHRM employees may submit a Privacy Act Request or contact the OHRM Office Manager to gain access to their information.
4.6	What are the procedures for correcting inaccurate or erroneous information?	OHRM employees can submit a Privacy Act Request or contact the OHRM Office Manager to correct inaccurate or erroneous information.

Section 5.0 Sharing and Disclosure

The following questions define the content, scope, and authority for information sharing.

#	Question	Response
5.1	Is information shared with internal office(s) or division (s)? • If yes, please identify the office(s) or division(s) and describe the information shared and for what purpose. • If no, please state "N/A" in the response section.	No. In the event of an emergency, if the OHRM executive in the employee's reporting structure is not available to notify the emergency contact, the emergency contact information will be retrieved from the access-controlled folder on the M:// Drive. Under these circumstances, an alternate OHRM executive may take on the responsibility of contacting the emergency contact. Access to the spreadsheet will be limited to the OHRM executive team and the OHRM Office Manager.

#	Question	Response
5.2	Is information shared with external (outside FHFA) agencies, organization(s), contractors, or other entities? For purposes of this Section, external organization(s) include Federal, state, and local government, and the private sector. • If yes, please identify the information shared, and for what purpose. If documents describe the information shared, please provide a copy. • If no, skip to Section 6.	No.
5.3	Is the sharing of PII outside the agency compatible with the stated purpose of the original information collection? • If yes, identify any applicable routine uses in the SORN listed in question 4.1 • If no, describe the legal authority that permits PII to be shared outside of FHFA.	No.

Section 6.0 Technical Access and Security

The following questions describe technical safeguards and security measures.

#	Question	Response
6.1	Will FHFA Office of Inspector General (OIG) or non-FHFA personnel (e.g., contractor personnel, regulated entity personnel) have access to the System/Collection and information contained therein? • If yes, how will they gain access to the System? • If no, how will the agency control access to and use of that information? Are there procedures or criteria documented in writing? If so, please describe.	No. Access to the spreadsheet will be limited to the OHRM executive team and the OHRM Office Manager.
6.2	Are there any conflicts of interest with respect to the System/Collection or information? If so, describe how those conflicts are addressed.	No.
6.3	Describe the type and frequency of training that is provided to users either generally or specifically that is relevant to the System/Collection.	All FHFA employees are required to undergo Security, Privacy, and Records and Information Management (RIM) training for use of FHFA systems at onboarding and annually thereafter. In addition, all FHFA users with elevated privileges receive specialized security training, and role-based privacy awareness training for those individuals whose work duties and responsibilities involve the collection, use, storage, access, or maintenance of PII.
6.4	Describe the technical/administrative safeguards in place to protect the data.	Data will be stored on the FHFA General Support System (GSS) and protected by the controls described in the FHFA GSS System Security and Privacy Plan (SSPP) and the GSS PIA. These controls include, but are not limited to, role-based

		access controls that restrict access to information based on Active Directory groups and permissions, auditing of file access and modification, data encryption, etc. The FHFA GSS is in the ongoing authorization phase of the Risk Management Framework and undergoes annual control assessments and reauthorization consistent with the Risk Management Framework.

7.0 Risk

The following questions describe the risk to the information within the system or collection.

#	Question	Response
7.1	Given the amount and type of information collected, what are the risks to an individual's privacy associated with collection of the data? Explain in detail how the loss or compromise of the information will/can affect an individual's privacy and describe how these risks are mitigated.	The risk to an individual's privacy if the data is lost or compromised is a misuse of the personal information of the employee and the employee's emergency contact.
7.2	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	There are minimal risks associated with the length of time the data is retained. The data is maintained for the length of time that the employee is employed within OHRM and is in accordance with the GRS. Access to this data is controlled and only provided as needed as described in this document.
7.3	Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.	N/A. Information is not shared externally.