Privacy Impact Assessment

Reasonable Accommodation System

June 2024

Contact

Greg Goldstein

Senior Agency Official for Privacy

Federal Mediation & Conciliation Service

250 E Street SW

Washington, D.C. 20427

Privacy@fmcs.gov

Abstract

The Federal Mediation and Conciliation Service (FMCS) Office of Information Technology (OIT) operates a current system of records titled "Reasonable Accommodation System." The system is intended to bring together a web-based, enterprise-wide, single point-of-entry reporting system. The system will include information that FMCS collects and maintains for applicants for employment and federal employees who request and/or receive reasonable accommodations for medical or religious reasons. The system will allow documenting and reporting all forms for compliance and accessibility activities and consistently track current status and progress towards meeting compliance requirements. The PIA is being conducted to determine any privacy issues with FMCS' employee information.

Overview

The FMCS Office of Human Resources (OHR) owns the Reasonable Accommodation System. The Reasonable Accommodation System ensures that electronic information technology acquired, developed, maintained, or used by FMCS for reasonable accommodation records are accessible to employees and prospective employees who request or receive reasonable accommodations or other appropriate modifications from FMCS for medical or religious reasons as mandated by Section 508 of the Rehabilitation Act Amended in 1998. Section 508 requires federal agencies to make all electronic information technology accessible to individuals and members of the public with disabilities.

OIT provides a centralized system to bring all various information together to allow OHR to manage and track the status of requests and progress towards meeting Section 508 compliance requirements. OIT's system administrator who has access on role-based permission accounts is restricted in accessing the system. The administrative account holder cannot see the personally identifiable information but may grant access or permission to other authorized FMCS employees.

Section 1. Characterization of the Information

1.1 What information is collected, used, disseminated, created, or maintained in the system? Are the types of information collected, used, maintained, and/or shared specified in its Privacy Notices?

The FMCS collects information from individuals who submit requests for the reasonable accommodation process. This information includes:

- Full name of the requester;
- Requester's status (applicant or employee);
- Requester's contact information (addresses, phone numbers, and email addresses);
- Employee's position title, grade, series, step;
- Date of the request;
- Description of the medical condition or disability and any medical documentation supporting the request;
- Description of the accommodation being requested;
- Description of religious belief and how it will impact the ability to comply with agency requirements and perform officials' duties;

- Supplemental medical records or medical certification documents in support of the request or determination;
- Description of previous requests for accommodation;
- Whether the request was granted, and if denied, the reason for the denial;
- Documentation of how the request was made;
- Documentation of any extenuating circumstances that prevent FMCS from meeting relevant timeframes;
- The sources of technical assistance consulted in trying to identify a possible reasonable accommodation;
- Any reports or evaluations prepared in determining whether to grant or deny the request; and
- Any other information collected or developed in connection with the request for a reasonable accommodation.

The types of information collected, used, maintained, and /or shared are specified in its Privacy Notices.

PII Mapping Components

The FMCS Reasonable Accommodation System consists of FMCS-0005 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by the FMCS Reasonable Accommodation system, FMCS-0005, and the functions that collect it are mapped below.

PII Mapped to Components				
Components	Does this function collect or store PII (Yes/No)	Type of PII	Reason for Collection of PII	Safeguards
Office of Human Resources	Yes	• Full names • Contact information including phone number, email, and address • Position, title, grade, series, step • Medical records or medical certification documents	The purpose for the collection of PII is to process and maintain religious and medical accommodation requests on applicants for employment, employees, and other individuals who participate in FMCS programs or activities who request or receive reasonable accommodations or other appropriate modifications from FMCS for medical or religious reasons.	Records are maintained in electronic and hard copy form on the agency's internal servers with restricted access to authorized Human Resources staff and designated deciding officials as determined by agency policy.

1.2 What are the sources of the information in the system?

The sources of information generated or collected are from applicants for employment, FMCS employees, contractors, former federal employees, medical providers or professionals, religious or spiritual advisors, and other individuals who participate in FMCS programs or activities who have requested religious and medical accommodations or other appropriate modifications from FMCS for medical or religious reasons.

1.3 How is the information collected?

The information is collected directly from the individuals submitting a request for religious and medical accommodations who participate in FMCS programs or activities and services via web, phone, or email.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

The purpose of the information is for FMCS to collect, process, and maintain religious and medical accommodations on applicants for employment, federal employees, and other individuals who participate in FMCS programs or activities who request and/or receive reasonable accommodations or other appropriate accommodations from FMCS for medical or religious reasons.

1.5 How will this information be checked for accuracy?

The accuracy is ensured by collecting the information from the source who must attest to the truthfulness of the information provided, including any documentation to support the request by the requester.

1.6 What specific legal authorities, arrangements, and agreements defined the collection of information?

The Executive Order 13164 requires each federal agency to establish effective written procedures for processing requests for reasonable accommodations. It ensures that agency's systems of recordkeeping track the processing of requests for reasonable accommodations and maintain the confidentiality of medical information received in accordance with applicable laws and regulations.

The FMCS is authorized to collect information under the following statutes: 29 U.S.C. 172, et seq.; Title VII of the Civil Rights Act of 1964, 42 U.S.C. 2000e, et seq.; 42 U.S.C. 12101; The Rehabilitation Act of 1973, 29 U.S.C. 701, 791, 794; E.O. 13164, as amended by E.O. 13478; E.O. 13548; E.O. 14043; 29 C.F.R. part 1605; 29 C.F.R. part 1614; 29 C.F.R. part 1615; and 29 C.F.R. part 1630.

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Principle of Purpose Specification: To inform information owners the reason why the religious and medical accommodation requests on applicants for employment, federal employees, and other individuals is being collected and the specific purposes for which it will be processed and maintained.

Principle of Minimization: FMCS limits collection of personal information to what is directly relevant and necessary to accomplish its specified purpose.

Principle of Individual Participation: FMCS protects personal data by adequate and reasonable security safeguards against such risks as loss or unauthorized access to data or information.

Principle of Data Quality and Integrity: FMCE ensures data or information collected is reliable and accurate i.e., the data is complete, consistent, and used for its intended purpose.

Risk Assessment: The main privacy concern is identifying potential events that may negatively impact individual's contact information.

Privacy Risk: The main privacy risk is the identification of an individual by their contact information. Another privacy risk is that the system will collect and maintain more information than is relevant and necessary to accomplish the Agency's mission.

Mitigation: The information in the system is private and confidential and only accessible to individuals on a need-to know basis. The system can allow or restrict access to system functions, data, and documents based upon user role and identity.

Section 2. Uses of the Information

2.1 Describe how the information in the system will be used in support of the program's business purpose.

The information stored in the system include reasonable accommodations for medical or religious reasons. FMCS collects and maintains records for applicants for employment and federal employees who participate in FMCS programs or activities who request or receive reasonable accommodations from FMCS for religious or medical reasons. FMCS will use this information to make determinations regarding reasonable accommodation requests.

2.2 What types of tools are used to analyze data and what type of data may be produced?

There are no special tools used to analyze data. The Office of Human Resources (OHR) or the Equal Employment Opportunity (EEO) Office may use the data collected to provide only aggregate data regarding requests, grants, and denials. It does not report using personally identifiable information. Authorized users may search requests by the name of the individual requesting the accommodation, the location of the employee, or the date of the request.

2.3 PRIVACY IMPACT ASSESSMENT: Use of the information

How is access to the PII determined? Access is determined by need-to-know and authorization from leadership.

Are procedures, criteria, controls, and responsibilities regarding access documented? Yes, all electronic processes are documented by the Office of Information Technology and maintained on their shared drives or secured in SharePoint.

Does access require manager's approval? Yes, all access must be granted by management approval.

Is access to the PII being monitored, tracked, or recorded? Yes, access to all data is monitored by the Office of Information Technology.

Who is responsible for assuring safeguards for the PII? Safeguards for PII are the responsibility of the managers of the Office of Human Resources and the Office of Information Technology.

Principle of Transparency: FMCS is transparent in the use of individual data as stated or described in the SORN.

Principle of Use of Limitation: FMCS uses PII collected solely for the purpose specified.

Risk Assessment: FMCS will evaluate the risk of a data breach in safeguarding religious or medical information.

Privacy Risk: There is a possible risk of misusing or mishandling collected information.

Mitigation: To mitigate this risk, only authorized users with account logins are allowed to access the records.

Section 3. Retention of Information.

3.1 What information is being retained?

FMCS retains all information previously listed in Section 1.1.

3.2 How long is information retained?

All records are retained and disposed of in accordance with General Records Schedule 2.3, issued by NARA. Records are updated as needed, retained for three years after separation and/or for the entirety of the employee's active employment, and destroyed by shredding or deleting.

3.3 Has the retention schedule been approved by the FMCS Records Office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule?

The retention schedule has been approved by the FMCS Records Office and NARA. The name of the records retention schedule is Employee Relations Records.

3.4 What are the procedures for the elimination of Sensitive Personal Information (SPI)?

The term "sensitive personal information", with respect to an individual, means any information about the individual maintained by an agency, including the following: (A) Education, financial transactions, medical history, and criminal or employment history. (B) Information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, or biometric records. SPI is minimized at the start by not asking for such information unless absolutely necessary to complete the system tasks. Additionally, information is protected by being kept on a secure server and limiting access to only those with need to know. Once the information has been used, it is removed from the servers so that public access is reduced or eliminated.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy of using PII for research, testing, or training?

The system is well designed to minimize the risk to privacy for using PII for research, testing, or training by adopting a protective and preventive mechanism to deprive unauthorized users of using PII by deploying SharePoint and Cloud-based services such as Zoom.gov and Microsoft teams that require a Multi-Factor Authentication (MFA) for system access.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of Information

Principle of Minimization: FMCS only collects PII that is directly relevant and necessary to accomplish its specified purposes and only retain PII for as long as necessary to fulfill its specified purposes. PII should be disposed of in accordance with FMCS records disposition schedules as approved by NARA.

Principle of Data Quality and Integrity: FMCS does, to the extend practical, ensure that PII is accurate, relevant, timely, and complete within the context of each use of the PII.

Risk Assessment: The systematic way of evaluating the potential risk of retaining records arising from the processing of data.

Privacy Risk: There is a possibility of retaining more information than necessary and retaining information longer than necessary.

Mitigation: FMCS applies NARA-approved records retention schedules to the information collected. Once the records meet the destruction date designated in GRS 2.3, FMCS will destroy the records by shredding or deleting.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure.

4.1 Which internal organizations is information shared or received? What information is shared or received, and for what purpose? How is the information transmitted or disclosed?

The internal organization which information is shared or received is with the OHR. OHR receives information previously listed in Section 1.1 to collect, store, and maintain records on applicants for employment, federal employees, and other individuals who participate in FMCS programs or activities who request or receive reasonable accommodations from FMCS for religious or medical reasons. This information is shared to enhance productivity and provide information relating to an individual's religious and medical requests within the Agency.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the risks associated with the sharing of information within FMCS. The risks include unauthorized personnel accessing the data, and release of information either intentionally or unintentionally.

What steps, if any, are currently being taken to mitigate those identified risks. The mitigation of the above risks includes the use of authorization and authentication measures previously identified and securing the data to prevent accidental release.

Risk Assessment: FMCS will evaluate the risk of a data breach in safeguarding religious or medical information.

Privacy Risk: It is anticipated that the information collected may be retained longer than its necessary.

Mitigation: The strategy adopted by FMCS to prevent privacy risks is by ensuring records are being protected by preventing unauthorized personnel from accessing records through necessary safeguards of personnel data and building a privacy-resilient workplace by deploying risk detection and remediation mechanisms to prevent access of documents.

Section 5. External Sharing/Receiving and Disclosure

5.1 With which external organizations (outside FMCS) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed to authorized entities, as is determined to be relevant and necessary, outside the FMCS as a routine use pursuant to 5 U.S.C. 552a(b)(3). Please see Section 4.1 for the information that is shared and the purpose.

The sharing of information outside of the agency is compatible with the original collection. It is also covered by an appropriate routine use in the SORN under 5 U.S.C 552a(b)(3) of the Privacy Act.

Describe how information is transmitted to entities external to FMCS and what security measures have been taken to protect it during transmission.

The transmission of information or electronic records to external entities occurs through a web browser to the internet or on the agency's internal drives which requires a Multi-Factor Authentication (MFA) for login. The security measures or mechanism in place are an antivirus and malware protection of the system to prevent data leakages or corruption of data and the encryption of transmitted information will protect the file from breaches in confidentiality and integrity of the data or information. The information must be transmitted on a secured network i.e WIFI which will require a strong password to access the network and to prevent any unauthorized personnel or intruder in accessing the network.

External Sharing/Receiving and Disclosure				
Program Office or IT System information is shared/received with	Reason why information is shared/received with the specified program or IT System	List the specific information types that are shared/received with the Program or IT System	List all legal authority, binding agreement, SORN routine use, etc. that permit external sharing	Method of transmission and measures in place to secure data
Reasonable accommodation information is not shared externally unless generally permitted under 5 U.S.C. 552a(b) of the Privacy Act or as a routine use pursuant to 5 U.S.C. 552a(b)(3).	The information shared within the IT system is used to process and maintain records of individuals who participate in FMCS programs or activities who request or receive reasonable accommodations or other appropriate modifications from FMCS for medical or religious reasons.	Reasonable accommodation information is not shared externally unless generally permitted under 5 U.S.C. 552a(b) of the Privacy Act or as a routine use pursuant to 5 U.S.C. 552a(b)(3).	All or a portion of the records or information contained in this system may be disclosed to authorized entities, as is determined to be relevant and necessary, outside the FMCS as a routine use pursuant to 5 U.S.C 552a(b)(3).	Records are transmitted in hard copy or electronic form and are stored in restricted locations only accessible to authorized Human Resources staff and designated deciding officials as determined by agency policy.

5.2 PRIVACY IMPACT ASSESSMENT: External Sharing/ Receiving and Disclosure

Risk Assessment: FMCS will evaluate the risk of a data breach in safeguarding religious or medical information.

Privacy Risk: There is significant risk in sharing medical or religious information outside the agency without proper authority.

Mitigation: The risk is mitigated by ensuring records are only accessible to authorized Human Resources staff and designated deciding officials as determined by Agency policy.

Section 6. Notice

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

Yes, there is a Privacy Act Statement on the Reasonable Accommodation Form, and a system of records notice was published in the Federal Register. The system of records notice for the Reasonable Accommodation SORN is here and the Privacy Act Statement is here.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

Information requested on the Reasonable Accommodation Form is required and failure to provide the requested information could result in FMCS' delay or inability to render a decision on a requested accommodation.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

FMCS collects information solely for the purpose of providing service based on the request of individuals. FMCS will not be able to respond or proceed with processing the request if an individual does not provide the appropriate supporting documentation or information.

6.4 PRIVACY IMPACT ASSESSMENT: NOTICE

Principle of Transparency: FMCS provides notice to individuals regarding its collection, use, and maintenance of PII.

Principle of Use Limitation: FMCS does not use or disclose personal information for purposes other than those which it has identified.

Risk Assessment: FMCS will evaluate the risk of a data breach in safeguarding religious or medical information.

Privacy Risk: There is the risk that individuals will not be given appropriate notice prior to collection of their information.

Mitigation: This risk is mitigated since the system provides notice at the onset of the collection process regarding the purpose of the collection, the routine uses of the disclosure of information, and the consequences for failure to provide the information. This risk is also mitigated since the notice of the collection of information is provided in the PIA available on the public facing website, the Privacy Act Statement on the Reasonable Accommodation Form, and by the notice in the *Federal Register* for the Reasonable Accommodation SORN.

Section 7. Access, Redress, and Correction

7.1 What are the procedures that allow individuals to gain access to their information?

If an employee would like access to their religious or medical accommodation information, they would send a request with the specific information needed to the resource mailbox at FMCSMedicalInfo@fmcs.gov. A copy of the requested information will be provided via email in an encrypted file.

In addition, other individuals must provide the following information for their records to be located and identified: (1) Full name, (2) Address, and (3) A reasonably identifying description of the record content requested. Requests can be submitted via fmcs.gov/foia/, via email to privacy@fmcs.gov, or via mail to FMCS, Privacy Office, 250 E Street, SW, Washington, DC 20427. Also, see 29 CFR 1410.3, Individual access requests, for more information.

7.2 What are the procedures for correcting inaccurate or erroneous information?

See 29 CFR 1410.6, Requests for correction or amendment of records, on how to contest the content of any records. Privacy Act requests to amend or correct records may be submitted to the Privacy Office at privacy@fmcs.gov, FMCS 250 E Street, SW, Washington, DC 20427. Also, see https://www.fmcs.gov/privacy-policy/.

7.3 How are individuals notified of the procedures for correcting their information?

The PIA and the notice on the *Federal Register* provides notice to individuals on how to correct their information.

7.4 If no formal redress is provided, what alternatives are available to the individual?

There is formal redress provided for the correction of inaccurate information.

7.5 PRIVACY IMPACT ASSESSMENT: Access, Redress, and Correction

Principle of Individual Participation: FMCS involves the individual in the process of using PII. FMCS seeks individual consent for the collection, use, dissemination, and maintenance of PII and provide mechanisms for appropriate access, correction, and redress regarding its use.

Risk Assessment: FMCS will evaluate the risk of a data breach in safeguarding religious or medical information.

Privacy Risk: An individual may not be aware of the process for accessing and/or correcting information.

Mitigation: To mitigate the risk, FMCS has provided a PIA on our public facing website and provided a notice in the *Federal Register*, so individuals are aware of the process for accessing and/or correcting information.

Section 8. Technical Access and Security

8.1 What procedures are in place to determine which users may access the system, and are they documented?

The owner of the system and leadership determines who may access it. IT then grants any electronic access necessary for the access.

8.2 Will FMCS contractors have access to the system and the PII? If yes, what involvement will contactors have with design and maintenance of the system? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

Yes, FMCS contractors may have access to the system regarding Reasonable Accommodations. All contractors must be authorized and maintain a Level 2 Public Trust clearance.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All FMCS users must undergo privacy awareness training and information security and awareness training before commencement of their job assignment. These trainings highlight the importance of

securing FMCS information, PII, and information systems, identifies roles and responsibilities employees have when accessing agency systems, defines a privacy breach and how to report a breach, provide tips to avoid breaches in information security, provide the basics about the Privacy Act, and describes Privacy Act resources available at FMCS.

8.4 Has Authorization and Accreditation (A&A) been completed for the system?

Yes, all applications that are used in the Reasonable Accommodation system have Authority to Operate (ATO)s on file with the Office of Information Technology and with Federal Risk and Authorization Management Program (FedRAMP®) as required.