Privacy Impact Assessment

Case Records SORN

January 22, 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 E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII).

The assessment is a practical method of evaluating privacy in information systems and collections and assures privacy issues have been identified and adequately addressed. The process is designed to guide FMCS system owners and developers in assessing privacy during the early stages of development and throughout the System Development Life Cycle (SDLC) to determine how their project will affect the privacy of individuals and whether the project objectives can be met while also protecting privacy.

Overview

The PIA ensures total compliance with laws and regulations governing privacy and demonstrates the FMCS's commitment to protect the privacy of any personal information the agency collects, stores, retrieves, uses, and shares. It is a comprehensive analysis of how the FMCS's electronic information systems and collections handle PII. The objective of the PIA is to systematically identify the risks and potential effects of collecting, maintaining, and disseminating PII and to examine and evaluate alternative processes for handling information to mitigate potential privacy risks.

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 information collected, used, maintained and/or shared in the system are as follows:

1) Requests for mediation or training completed by parties to include the Agency Form F-7, available on www.fmcs.gov . The information collected on the form includes contact information for parties requesting services.

2) Case processing documents and documents sent to or from parties to a mediation: Agency confirmation letters sent to parties assigning mediators to cases or trainings, mediation agreements, ethics documents concerning mediator involvement and authorizations to participate, and reports and invoices regarding mediations and training.

PII Mapping Components

FMCS Case Records System consists of FMCS-0004 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by FMCS Case Records, FMCS-0004, 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 Client Services	Yes	• Full Name • Full Addresses • Phone number and extension • Email • Title	The records in this system are used to process, track, review, and evaluate requests for mediation, training, and another alternative dispute resolution services. Records from this system may also be used for training, presentation, and research purposes, and for the preparation of internal agency reports, the agency's budget requests, and reports to Congress.	Case records are maintained in electronic form on the agency's internal drives both requiring username and password for login. Case records and agreements are accessible to restricted FMCS personnel or contractors who require access.

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

The primary source of information in the system are FMCS clients who are parties to labor agreements/disputes, mediations, or those requesting FMCS services submit notices and requests to FMCS. FMCS personnel create reports, status updates, and other internal processing records on case progress and management. The National Labor Relations Board and the Federal Labor Relations Authority provide documents to FMCS regarding initial contracts.

1.3 How is the information collected?

The information is collected through an FMCS online portal. The notice of dispute filed with FMCS is submitted electronically via a platform provided by the agency.

The agency's internal drives, SharePoint, Outlook, Cloud-based services such as Zoom.gov and Microsoft Teams, and a case records management system are used to store electronic case tracking information, electronic case files (including mediation agreements), and recorded meetings and trainings.

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

The purpose of the information in the system is used to process, track, review, and evaluate requests for mediation, training, and other alternate dispute resolution services. Information in the system may be used for training, presentation, research purposes, and used in preparation of internal agency reports, the agency's budget requests, and reports to Congress.

1.5 How will this information be checked for accuracy?

The information is provided by the public. Therefore, the accuracy is ensured by collecting the information from the source, who must attest to the truthfulness and fairness of the information they provide including any documentation. Information submitted on the F-7 form is also verified by FMCS employees.

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

Federal Mediation and Conciliation Service, 29 U.S.C 172, et seq.; The National Labor Relations Act, 29 U.S.C. 151, et seq.; Administrative Dispute Resolution Act, 5 U.S.C. 571-584; Negotiated Rulemaking Act of 1990, 5 U.S.C. 561-570; and the Federal Labor Relations Act, 5 U.S.C. 7119.

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Principle of Purpose Specification: The FMCS case records should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose for which records, or data is intended to be used for.

Principle of Minimization: The FMCS should only collect PII that is directly relevant and necessary to accomplish its specified purposes and only retain PII for as long as necessary to fulfil its specified purposes. The PII should be disposed of in accordance with FMCS disposition schedules as approved by the National Archives and Records Administration (NARA).

Principle of Individual Participation: The FMCS involves the individual in the process of using or generating case records. The agency also seeks individual consent for the collection, use, dissemination, and maintenance of PII.

Principle of Data Quality and Integrity: The FMCS ensures that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

Risk Assessment: The main privacy concern is the identification of potential events that may negatively impact an individual's contact information presented.

Privacy Risk**:** There is a privacy risk that the system will collect and maintain more information than is relevant and necessary to accomplish the agency's mission.

Mitigation: This risk is mitigated. FMCS will only collect information regarding the case records management system to enable mediators and managers to manage cases, manage reporting requirements, provide data for research and training, store recorded trainings and meetings, and collect information on Agency operations which provides for a minimal collection of PII. Additionally,

FMCS provides the statutory protections afforded under the Privacy Act, along with the privacy tenets in the Fair Information Practice Principles and strives to only collect personal information that is necessary to accomplish the agency's mission.

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 purpose of the system is for processing, storing, and maintaining FMCS case records, notices, and agreements that interact with agency's internal drives, SharePoint, Outlook, and cloud-based services and store them in a secure repository which allows for search, retrieval, and view when necessary.

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

There is not a special tool used to analyze the data. The reporting is simple, providing only a running total of individuals requesting information. A report does not use PII but allows searching of requests by an assigned person responsible for solving and closing a request.

2.3 PRIVACY IMPACT ASSESSMENT: Use of the information

How is access to the PII determined? Access is determined by need. Need is determined by a user's ability to complete their tasks.

Are procedures, criteria, controls, and responsibilities regarding the access documented? All procedures, controls and responsibilities are documented and maintained in a secure location by IT.

Does access require manager approval? Yes, access is determined by job description and given with management approval.

Is access to the PII being monitored, tracked, or recorded? Yes, the system should be capable of monitoring, tracking, or recording PII information.

The Office of Information Technology is responsible for assuring safeguards and management of the information and information systems.

Principle of Transparency: This is the process whereby any information shared to the public is concise, easily accessible, easy to understand, and free from ambiguity and stated in plain language.

Principle of Use Limitation: This is the process whereby public or personal data should not be disclosed, made available or otherwise used for purposes other than those specified except with the consent of the data subject or by the authority of law.

Risk Assessment: This ensures that the agency accurately measure and manage the risk associated with handling public information and keeps the agency compliant with the global or government data protection regulations.

Privacy Risk: This is the process whereby the system will collect and maintain more information than is relevant and necessary to accomplish the agency's mission.

Mitigation: This is the process whereby a strategy is adopted by not storing or processing private or public sensitive information unprotected. The agency should take cognizance of every bit of public

information that they get and weigh the benefit of having this information against the risk of losing it or the information made available to unauthorized personnel.

Section 3. Retention of Information

3.1 What information is being retained?

The case records identified in Section 1.1 are being retained.

3.2 How long is information retained?

All case records are retained and disposed of in accordance with General Records Schedule (GRS) 1.1 and 4.2, issued by NARA.

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 record retention schedules are Financial Management and Reporting Records, GRS 1.1, and Information Access and Protection Records, GRS 4.2, issued by NARA.

3.4 What are the procedures for the elimination of Serial Peripheral Interface (SPI)?

The Serial Peripheral Interface is a full- duplex synchronous serial communication, which means that data can be simultaneously transmitted from both directions. The process is to transfer the data without any interruption and so many bits can be sent or received at a time in this protocol. The procedure for the elimination of SPI is by adopting a common serial port, the kind with TX and RX lines called “Asynchronous.” Asynchronous port has no control over when data is sent or any guarantee that both sides are running at precisely the same rate. Since computer systems normally rely on everything being synchronized to a single clock, this can be a problem when two systems with slightly different clocks try to communicate with each other. To work around this problem, asynchronous serial connections add extra start and stop bits to each byte which help the receiver sync up to data as it arrives.

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 of using PII for research, testing, or training by adopting a protective and preventive mechanism to deprive unauthorized users by deploying SharePoint, Outlook, and Cloud-based services such as Zoom.gov and Microsoft teams, requiring a username and password for system access.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Principle of Minimization: The FMCS should only collect data or information that is directly relevant and necessary to accomplish the agency’s purpose and only retain the information as long as necessary to support the system for its intended purpose. Case records should be disposed of in accordance with GRS 1.1 and 4.2 issued by NARA.

Principle of Data Quality and Integrity: The FMCS case records should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete within the context of each use of the records.

Risk Assessment: This assists the agency to analyze and assess the privacy risks associated with the retention of records for individuals arising from the processing of their data.

Privacy Risk: There is a risk that unauthorized individuals may access the data for mischievous purposes which can lead to vicarious liability on the agency.

Mitigation: This risk is mitigated. The agency will take all reasonable steps necessary to maintain the security of all data collected, and will protect the data from inappropriate, unauthorized, or unlawful access, use, disclosure, or destruction.

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 organizations which information is shared or received are the Office of Client Services, IT, and all the Field Offices.

Information is transmitted or disclosed through the agency's internal drives, SharePoint, Outlook, Cloud-based services such as Zoom.gov and Microsoft Teams, and a case records management system which are used to store electronic case files (including mediation agreements), and recorded meetings and trainings, permitting the accurate and timely collection, retrieval, and retention of information maintained by offices of the agency.

The information FMCS shares or receives is listed in Section 1.1. The case records management system is used to process, track, review, and evaluate requests for mediation, training, and other alternate dispute resolution services. Records from this system may be used for training, presentation, research purposes and used in the preparation of internal agency reports, the agency's budget requests, and reports to Congress.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

There are various risks associated with the sharing of information within FMCS such as information security risks, compliance risks, and regulatory risks. Information security risk leads to data leakages and unwanted or unauthorized personnel having access to information. Compliance risk leads to failure to comply with laws, regulations, and standards. Regulatory risk leads to new regulations that threaten the agency business model.

What steps, if any, are currently being taken to mitigate those identified risks? The system is being assessed through agency internal drives or SharePoint using assigned username and password for preventive measures for unauthorized user to assess the records.

Risk Assessment: This assists the agency to analyze and assess the privacy risks for individuals arising from the processing of their data.

Privacy Risk: There is a risk of sharing information with individuals without a valid need-to-know.

Mitigation: The centralization of data using a web application has mitigated most of the risks associated with the inadvertent release of information.

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). The information FMCS shares/receives is listed in Section 1.1. The case records management system is used to process, track, review, and evaluate requests for mediation, training, and other alternate dispute resolution services. Records from this system may be used for training, presentation, research purposes, and used in the preparation of internal agency reports, the agency's budget requests, and reports to Congress.

The case records may be received electronically and in hardcopy form from FMCS clients. The hardcopy forms are then scanned and stored electronically on FMCS servers for access for authorized personnel or users using their username and password. FMCS clients submit the information directly through the public webpage.

Is sharing the information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of FMCS.

Yes, it 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 username and password for login. The security measures or mechanism in place are 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
	The information shared within the IT system is used to make requests	The information FMCS receives/shares is	Federal Mediation and Conciliation Service, 29 U.S.C.	The case records may be received electronically and in

	for mediation or training programs and case processing documents for dispute resolutions among parties within and outside agencies.	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.	172, et seq; The National Labor Relations Act, 29 U.S.C. 151, et seq; Administrative Dispute Resolution Act, 5 U.S.C 571-584; Negotiated Rulemaking Act of 1990, 5 U.S.C. 561-570; and the Federal Labor Relations Act, 5 U.S.C. 7119. The 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).	hardcopy form from FMCS clients. The hard copies are then scanned and stored electronically on FMCS servers for access for authorized personnel or users using their username and password. FMCS clients submit the information directly through the public webpage.

5.2 PRIVACY IMPACT ASSESSMENT: External Sharing/Receiving and Disclosure

Risk Assessment: It is the identification of threat sources, vulnerabilities, and determination of the likelihood of occurrence to analyze and assess privacy risks for external sharing of information on individuals arising from the processing of their data and information.

Privacy Risk: There is a significant risk in sharing information outside the scope of the Case Records SORN or without the authorized permission for disclosures. It can lead to violation of civil or criminal laws or regulations.

Mitigation: The risk is mitigated by ensuring case records are only accessible to authorized personnel. Electronic records are stored on the agency's internal servers with restricted access to authorized personnel.

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 are Privacy Act Statements on forms and a system of records notice was published in the Federal Register. The system of records notice can be found here: FMCS Case Records SORN. The Privacy Act notice on forms can be found here: Privacy Act Statement for F-7 form.

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

No, individuals do not have the opportunity or right to decline to provide information. As stated in the Privacy Act Statement, it is authorized and enforced by law. Failure to provide the requested information could result in FMCS's delay or inability to provide services. To receive mediation services, those requesting mediations must provide the information requested in the F-7 form.

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

Yes, as captured in the Privacy Act Statement on the form, individuals consent to the use of the information in accordance with the Case Records SORN and as needed to receive mediation services from FMCS.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Principle of Transparency: The FMCS is transparent and provide notice to individuals on the collection, use, dissemination, and maintenance of their case records or PII. The technologies or systems processing case records and PII must be described in the Case Records SORN.

Principle of Use Limitation: The agency uses case records and PII solely for the purposes specified in the notice.

Risk Assessment: This assists the agency to analyze and assess the risks in the notice provisions for individuals from the processing of their data.

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

Mitigation: The risk is mitigated at the outset of the collection process regarding the purpose of the collection, the routine uses of the disclosure of information, and the consequences for a failure to provide the information. The notice of the collection of information is provided through the PIA for Case Records, the Privacy Act Statement on forms, and the Case Records SORN.

Section 7. Access, Redress, and Correction

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

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 the Privacy Office at FMCS, 250 E Street, SW, Washington, D.C. 20427. For more information, see 29 CFR 1410.3.

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

Requests for correction or amendment of records may be submitted to the Privacy Office at privacy@fmcs.gov or via mail to the Privacy Office at FMCS, 250 E Street, SW, Washington, D.C. 20427. For more information, visit https://www.fmcs.gov/privacy-policy/ and see 29 CFR 1410.6.

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

The PIA for Case Records and the Case Records SORN provides notice to individuals on how to correct their information.

7.4 If no 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: This assists the agency to analyze and assess the privacy risks for individuals in accessing, correcting, and redressing information.

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

Mitigation: To mitigate the risk, individuals may review the PIA for Case Records and the Case Records SORN.

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 case records and agreements are only accessible to restricted FMCS personnel or contractors who require access. The Office of Information Technology grants access to the system for FMCS employees. Access to the system may be granted in varying degrees of permissions: read-only or editing permissions. Non-supervisory employees may only have editing permissions for assigned cases.

8.2 Will FMCS contractors have access to the system and the PII? If yes, what involvement will contractors have with the 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 do have access to the system regarding case records notice or case processing documents, provided that access is granted to such contractors, and it is appropriate for assigned duties and responsibilities. The system covers current Federal employees or contracted personnel. FMCS contractors are fully engaged in the design, development, and maintenance of the system. All contractors accessing FMCS data are required to possess and maintain a minimum Tier 2 Public Trust clearance and sign an NDA before accessing any systems or FMCS data.

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?

The system is hosted in Dynamics365, which has a federal A&A put in place by Microsoft. In the future, it will be hosted by Salesforce and an A&A will be completed.