# Privacy Impact Assessment (PIA)

for the

# Department Medallia, Inc. – Medallia GovCloud (EDMedallia)

# May 18, 2022

**For PIA Certification Updates Only:** This PIA was reviewed on **Enter date** by **Name of reviewer** certifying the information contained here is valid and up to date.

## Contact Point

**Contact Person/Title:** Kimberly Ferguson/Information System Security Officer
**Contact Email:** Kimberly.Ferguson@ed.gov

## System Owner

**Name/Title:** Pardu Ponnapalli/Information System Owner
**Principal Office:** Federal Student Aid (FSA)

**Please submit completed Privacy Impact Assessments to the Privacy Office at privacysafeguards@ed.gov**

*Please complete this **Privacy Impact Assessment (PIA)** on how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document.*
***If a question does not apply to your system, please answer with N/A.***

## 1. Introduction

**1.1.** Describe the system including the name, acronym, and a brief description of the program or purpose for the system.

Department Medallia, Inc. - Medallia GovCloud (EDMedallia) is a cloud-based commercial-off-the-shelf (COTS) product that Federal Student Aid (FSA) will add to the Digital Customer Care (DCC) system boundary. Medallia is software that analyzes customer feedback and sentiments through mechanisms such as customer satisfaction surveys on websites. The data/analysis presented by Medallia can be used to identify improvements of evaluated FSA digital solutions to address customer pain points. The Medallia software consolidates the data that will be used to perform analysis of the FSA customer experience through customized dashboards and reports. EDMedallia ingests and consolidates feedback data from interactions with FSA end-users within the digital platform. Text analytics is performed in the Medallia back-end to identify trends and patterns based on aggregate survey data that is received. The output is presented to FSA users via reports and dashboards to facilitate the identification of pain-points/improvements to FSA digital assets. Additionally, EDMedallia will use open-response feedback to identify improvements in digital assets. EDMedallia uses multiple types of configurable surveys that can include criteria such as amount of time spent on a page, when a certain transaction is completed, and number of pages visited.

EDMedallia introduces a centralized feedback solution for FSA's DCC system. Medallia will aggregate end-user feedback collected from customer interactions on StudentAid.gov website, myStudentAid mobile application pages, and the Business Process Operations (BPO) customer service feedback including by ingesting interactive voice response (IVR) customer satisfaction data. After interactions with customer care agents within the BPOs, feedback is requested from the customer. That feedback will be presented via a Medallia survey, and the results of the survey will be ingested and analyzed by EDMedallia. FSA customer feedback collected through DCC's existing feedback channels (including the Virtual Assistant, Feedback Center, and social media) will be ingested into EDMedallia for a comprehensive view of FSA's customers' digital interactions. When FSA users log into the EDMedallia platform, they are presented with dashboards and reports that show the output of the text analytics run against FSA's customer feedback responses. All surveys for the FSA implementation are digital, either

a pop-up on the screen or an email generated by Medallia after select transactions are completed.

**1.2.** Describe the purpose for which the personally identifiable information (PII)[1] is collected, used, maintained or shared.

PII including first names and email addresses are collected and maintained within EDMedallia. This data is used to generate personalized emails to FSA customers when requesting feedback on their experience with select digital experiences. Age ranges, city, and ZIP codes will be also be collected and used to provide aggregate reporting that will aid FSA's ability to craft improved communications to key customer segments such as high school students, university/college students, borrowers, etc.

Is this a new system, or one that is currently in operation?

New System

**1.3.** Is this PIA new, or is it updating a previous version?

New PIA

The COTS product Medallia was acquired for use within the existing DCC system, therefore a new PIA is required.

**1.4.** Is the system operated by the agency or by a contractor?

Contractor

**1.4.1.** If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

☐ N/A

Yes

[1] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. OMB Circular A-130, page 33

## 2. Legal Authorities and Other Requirements

***If you are unsure of your legal authority, please contact your program attorney.***

**2.1.** What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system? Please include name and citation of the authority.

The authority to collect information for EDMedallia is based on the Higher Education Act (HEA) of 1965, as amended. Sections 483 and 484 of the Higher Education Act of 1965, as amended.

**SORN**

**2.2.** Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification?

Yes

For select interactions within the DCC, when an authenticated user completes an action the Management ID (MDMID) will be included with the data payload passed to Medallia. Medallia will issue a data call to the Person Master Data Management (pMDM) system to retrieve the first name and email address of that user to support the generation of an email requesting feedback.

**2.2.1.** If the above answer is **YES,** this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).[2] Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

☐ N/A

Federal Student Aid Application File (18-11-01). October 29, 2019. 84 FR 57856-57863. https://www.federalregister.gov/documents/2019/10/29/2019-23581/privacy-act-of-1974-system-of-records

Common Origination and Disbursement System (18-11-02). August 16, 2019. 84 FR 41979-41987. https://www.federalregister.gov/documents/2019/08/16/2019-17615/privacy-act-of-1974-system-of-records

[2] A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED. https://connected.ed.gov/om/Documents/SORN-Process.pdf

National Student Loan Database System (18-11-06). September 9, 2018. 84 FR 47265-47271. https://www.federalregister.gov/documents/2019/09/09/2019-19354/privacy-act-of-1974-system-of-records

Customer Engagement Management System (CEMS) (18-11-11). June 13, 2018. 83 FR 27587-27591. https://www.federalregister.gov/documents/2018/06/13/2018-12700/privacy-act-of-1974-system-of-records

Common Services for Borrowers (CSB) (18-11-16). September 2, 2016. 81 FR 60683 https://www.federalregister.gov/documents/2016/09/02/2016-21218/privacy-act-of-1974-system-of-records

**2.2.2.** If the above answer is **NO**, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.

☑ N/A

**Records Management**
**If you do not know your records schedule, please consult with your records liaison or send an email to RMHelp@ed.gov**

**2.3.** What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

EDMedallia follows the retention schedule under General Records Schedule (GRS) 6.5: Public Customer Service Records. The records are considered temporary and will be destroyed 1 year after resolution, or when no longer needed for business use, whichever is appropriate.

**2.4.** Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule?

Yes

## 3. Characterization and Use of Information

**Collection**

**3.1.** List the specific PII elements (e.g., name, email, address, phone number, date of birth, Social Security, etc.) that the system collects, uses, disseminates, or maintains.

PII including first names and email addresses are collected and maintained within EDMedallia. This data is used to generate personalized emails to FSA customers when requesting feedback on their experience with select digital experiences. Age ranges, city, and ZIP codes are also be collected and used to provide aggregate reporting that will aid FSA's ability to craft improved communications to key customer segments such as high school students, university/college students, borrowers, etc.

For select interactions within the DCC, when an authenticated user completes an action the MDMID assigned to the individual will be included with the data payload passed to Medallia. Medallia will issue a data call to the Person Master Data Management (pMDM) system to retrieve the first name and email address of that user to support the generation of an email requesting feedback

**3.2.** Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2?

Yes

The information collected is the minimum necessary to achieve the purpose of facilitating and analyzing customer satisfaction surveys. Contact information, such as the individual's name and email address is used to communicate with individuals who have been selected to take a customer satisfaction survey. Age ranges, city, and ZIP codes will be used to provide aggregate reporting that will aid FSA's ability to craft improved communications to key customer segments such as high school students, university/college students, borrowers, etc.

**3.3.** What are the sources of PII collected (e.g., individual, school, another agency, commercial sources, etc.)?

PII is collected directly from students and borrowers from customer interactions on the StudentAid.gov website. FSA customer feedback collected through DCC's existing feedback channels (including the Virtual Assistant, Feedback Center, and social media) will be ingested into EDMedallia for a comprehensive view of FSA's customers' digital interactions.

**3.4.** How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, web page, database, etc.)?

PII is collected through electronic customer satisfaction surveys. Existing PII maintained on DCC is also pulled from Person Master Data Management (pMDM), which is stored in the Common Origination & Disbursement (COD) system.

**3.5.** How is the PII validated or confirmed to ensure the integrity of the information collected?[3] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

For select actions performed on the FSA website, a request for feedback will be generated via email. Prior to each email, a data call will be made to pMDM to validate the first name and email address of the customer based on their MDMID.

**Use**

**3.6.** Describe how the PII is used to achieve the purpose stated in Question 1.2 above.

PII is used while generating personalized emails to FSA customers when requesting feedback on their experience with select digital interactions.

**3.7.** Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

No

**3.7.1.** If the above answer is **YES,** what controls are in place to minimize the risk and protect the data?

☑ N/A

**Social Security Numbers**

*It is the Department's Policy that, in order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.*

[3] Examples include restricted form filling, account verification, editing and validating information as it's collected, and communication with the individual whose information it is.

**3.8.** Does the system collect Social Security Numbers? Note that if the system maintains Social Security Numbers but does not explicitly collect them, answer 3.8.1 to address the purpose for maintaining them.

No

**3.8.1.** If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.

☑ N/A

**3.8.2.** Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.

☑ N/A

## 4. Notice

**4.1.** How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA,)? If notice is not provided, explain why not.

Direct notice, prior to the initial collection of PII, is provided during the FAFSA application process at studentaid.ed.gov when PII is collected by the Central Processing System (CPS). The DCC website (Studentaid.gov) provides additional detailed notice in its privacy policy referenced in question 4.2. Additionally, the Medallia surveys include links to the privacy policy referenced in question 4.2.

**4.2.** Provide the text of the notice or the link to the webpage where the notice is posted if notice is provided other than by SORN or PIA.

☐ N/A

The privacy policy for StudentAid.gov and the myStudentAid mobile app contains the following language:

"After interacting with Federal Student Aid (e.g., visiting StudentAid.gov, contacting us, or receiving communication from us), you may be asked to participate in a survey conducted by an authorized third party, Medallia. Your participation is voluntary. If you previously provided contact information to us, we may follow up with you in response to a survey you submit in order to resolve your issue or get more information about your

interaction. Survey data is retained as long as needed to conduct service recovery, permit accurate analysis, produce summary reports, and monitor overall trends. If you choose not to participate in the survey, you are not prevented from using the Federal Student Aid services in any other way. If you wish to provide feedback without taking the survey, you may use our Feedback Center. If you have an immediate concern, please refer to the "Contact Us" section."

Additionally, the Medallia surveys include links to the privacy policy referenced above.

**4.3.** What opportunities are available for individuals to consent to uses (including new uses of previously collected PII), decline to provide PII, or opt out of the project?

The borrower has the opportunity to choose not to complete a survey and therefore declines to provide PII.

**4.4.** Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practice, policy, or activities that affect the PII and privacy to ensure that individuals are aware of and can consent to, where feasible, these changes?

Yes

## 5. Information Sharing and Disclosures

### Internal

**5.1.** Will PII be shared internally with other ED principal offices? If the answer is **NO**, please skip to Question 5.4.

No

**5.2.** What PII will be shared and with whom?

☑ N/A

**5.3.** What is the purpose for sharing the specified PII with the specified internal organizations?

☑ N/A

### External

**5.4.** Will the PII contained in the system be shared with external entities (e.g., another agency, school district, the public, etc.)? If the answer is **NO**, please skip to Question

6.1.

No

**5.5.** What PII will be shared and with whom? List programmatic disclosures only.[4]
**Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose**.

☑ N/A

**5.6.** What is the purpose for sharing the PII with the specified external entities?

☑ N/A

**5.7.** Is the sharing with the external entities authorized?

☑ N/A

Click here to select.

**5.8.** Is the system able to provide and retain an account of any disclosures made and make it available upon request?

☑ N/A

Click here to select.

**5.9.** How is the PII shared with the external entity (e.g., email, computer match, encrypted line, etc.)?

☑ N/A

**5.10.** Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?

☑ N/A

Click here to select.

**5.11.** Does the project place limitation on re-disclosure?

☑ N/A

[4] If this information is covered by Privacy Act System of Records Notice (SORN) please list only relevant programmatic disclosures listed under the Routine Uses section.

Click here to select.

## 6. Redress

**6.1.** What are the procedures that allow individuals to access their own information?

If an individual wishes to access the content of a record in this system of records, he or she should contact the system manager full name, address, and telephone number to distinguish between individuals with the same name. The individual must meet the requirements in 34 CFR 5b.5, including proof of identity.

**6.2.** What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

If an individual wishes to contest the content of a record in this system of records, he or she should contact the system manager full name, address, and telephone number to distinguish between individuals with the same name, identify the specific items to be changed; and provide a written justification for the change. Requests to amend a record must meet the requirements of the regulations in 34 CFR 5b.7.

**6.3.** How does the project notify individuals about the procedures for correcting their information?

Individuals are notified of the procedures for correcting their information through the publication of this PIA and through the SORNs referenced in question 2.2.1.

## *7.* Safeguards

***If you are unsure which safeguards will apply, please consult with your ISSO.***

**7.1.** Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible?

Yes

**7.2.** Is an Authorization to Operate (ATO) required?

Yes

**7.3.** Under NIST FIPS Pub. 199, what is the security categorization of the system: **Low, Moderate, or High?**

☐ N/A

Moderate

**7.4.** What administrative, technical, and physical safeguards are in place to protect the information?

The Department and FSA have developed policies and procedures to address technical, administrative and physical safeguards.

Medallia is responsible for the security of all the data within the environment. All application data are encrypted at rest and in transit. Any contractor access to a Medallia application with PII occurs after FSA users' security clearance and customer on-boarding process. This requires any such person to attend customer specific security and privacy training.

Additionally, all users accessing the system are given unique user identification. The Department requires the enforcement of a complex password policy and two-factor authentication. In addition to the enforcement of the two-factor authentication and complex password policy, users are required to change their password at least every 90 days in accordance with the Department's information technology standards. Users of the application are allowed to browse only the information they have been given explicit access to. Configuration of the user roles will be managed by FSA. The only users with broad access to the application are users assigned to the administration role. FSA users can control which users are assigned this role.

In accordance with the Federal Information Security Management Act of 2002 (FISMA), as amended by the Federal Information Security Modernization Act of 2014, every FSA system must receive a signed ATO from a designated FSA official. The ATO process includes a rigorous assessment of security controls, a plan of actions and milestones to remediate any identified deficiencies, and a continuous monitoring program.

**7.5.** Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by Federal law and policy?

Yes

**7.6.** Has a risk assessment been conducted where appropriate security controls to protect against that risk have been identified and implemented?

Yes

**7.7.** Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the security controls continue to work properly at safeguarding the PII.

Monitoring, testing, and evaluation are ongoing as FSA follows the Department's Lifecycle Management framework and takes part in the ATO process which includes a rigorous assessment of the security and privacy controls and potential plans of actions and milestones to remediate any identified deficiencies. Additionally, the EDMedallia application is scanned regularly using automated tools to detect vulnerabilities. The results of the vulnerability scans are reviewed and addressed at the application and infrastructure levels. Annual security assessments are conducted as self-assessments and independent assessments. Intrusion detection and monitoring systems are employed to review accesses and modifications and detect anomalies. Changes are captured and reviewed in audit logs for all software components.

## 8. Auditing and Accountability

**8.1.** How does the system owner assess and ensure that the PII is used in accordance with stated practices in this PIA?

The system owner included the FSA Privacy program throughout the development of this new system. Since this is a public-facing system with multiple backend systems, the system owner ensures consistency and relevancy with the other relevant PIAs and SORNs.

The system owner ensures the information is used in accordance with stated practices by confirming the privacy risks are properly assessed, ensuring Privacy Act records are maintained in accordance with the provisions of the Federal Records Act, Departmental policies, the Privacy Act and the published SORN, ensuring appropriate security and privacy controls are implemented to restrict access, and to properly manage and safeguard PII maintained within the system. The system owner participates in all major security and privacy risk briefings, meets regularly with the information system security officer, and participates in FSA's Lifecycle Management Methodology, which addresses security and privacy risks throughout the system's life cycle. Additionally, the system owner regularly reviews signed agreements that govern data use between organizations, such as system of records notices, memorandums of understanding, and interconnection security agreements.

**8.2.** Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?

Yes

**8.3.** What are the privacy risks associated with this system and how are those risks mitigated?

Privacy risks associated with EDMedallia include unencrypted data being transmitted, lost, stolen, or compromised. Data breaches involving PII are potentially hazardous to both individuals and organizations. Individual harm may include embarrassment or inconvenience. Organizational harm may include a loss of public trust, legal liability, or remediation costs.

The risks are mitigated by the above-mentioned safeguards, limiting access to only those with a legitimate need to know, and working closely with the security and privacy staff at the Department. To further mitigate this risk, the following safeguards have been implemented:

- Monthly vulnerability scans
- Annual contingency plan test
- Annual or ongoing security assessments

Risks are also mitigated by updating security patches per the patch scheduling and updating devices operating software, amongst other software. System patching is performed monthly, and scans are run on the production environment each month in support of the monthly patching cycle. Collecting the minimum PII necessary to achieve the system's purpose also mitigates privacy risks.