

U.S. Department of Education Federal Student Aid



START HERE
GO FURTHER
FEDERAL STUDENT AID[®]

Financial Partners Data Mart (FPDM) Privacy Impact Assessment

Version 1.1

12/03/2009



Contents

1. Introduction.....	4
2. Responsibility.....	5
2.1. Revisions.....	5
3. Privacy Notices for Websites	6



Revision History

Version #	Date	Author	Revision(s) made	Approved by
1.0	11/23/2009	Don McComas	Document Creation	
1.1	12/15/2009	Don McComas	Incorporate revisions per client feedback	

* Define whether change is an addition, modification, deletion, or initial release



1. Introduction

The E-Government Act of 2002 put forth new reporting requirements for personal privacy information. The purpose of the mandate is to maintain and increase the integrity with which public information is handled by the government. Section 208 of the E-Government Act requires Federal Student Aid identify which systems collect information in identifiable form about the general public. To meet the objective, Federal Student Aid requires each system complete a Privacy Impact Assessment.



2. Responsibility

The System Security Officer is responsible for ensuring the team completes the attached Privacy Impact Assessment Questionnaire. The Privacy Impact Assessment should be filed electronically in the Security Library (Public Folder) for the particular Major Application, Minor Application, or General Support System for which the system resides.

2.1. Revisions

The Privacy Impact Assessment should be revised/updated when there has been a significant change in the collection or flow of data (e.g., new uses or disclosures of information, incorporation into the system of additional items of information in identifiable form, etc.).

The following list identifies types of identifiable information captured in the Privacy Impact Assessment:

- **Conversions** -- when converting paper-based records to electronic systems;
- **Anonymous to Non-Anonymous** -- when functions applied to an existing information collection change anonymous information into information in identifiable form;
- **Significant Management Changes** -- when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system;
- **Significant Merging** -- when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated;
- **New Public Access** -- when user-authenticating technology (e.g., password, digital certificate) is newly applied to an electronic information system accessed by members of the public;
- **Commercial Sources** -- when agencies incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources (merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);
- **New Uses** -- when agencies work together on shared functions involving new uses or exchanges of information in identifiable form, such as the cross-cutting e-government initiatives; in such cases, the lead agency should spearhead the PIA activity.



3. Privacy Notices for Websites

In addition to the Privacy Impact Assessment, the E-Government Act of 2002 also mandates that Privacy Notices must be placed on agency websites; including the principal website and pages where substantial information in identifiable form is collected. The web page author must include or hyperlink to a Privacy Notice on any form or page where a user enters personal information. Most of the content of the Privacy Notice comes from responses to the Privacy Impact Assessment Questionnaire. Specifically, the Notice must include:

- What information is being collected;
- Why the information is being collected;
- The intended use of the information;
- With whom (ex. Other agencies) the information will be shared (if at all);
- What notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
- How the information will be secured; and
- The rights of the individual under the Privacy Act and other laws relevant to protection of the privacy of an individual. (This section could include the following, “If you have any additional questions regarding your Privacy Act rights as related to the information we collect, please contact *address of SSO or someone in Dept of Ed.*”)

• Please see the Department of Education’s Privacy Policy for ed.gov as an example, website address is found at:

- <http://www.ed.gov/notices/privacy/index.html>

System Name: Financial Partners Data Mart (FPDM)

System Owner: Keith Wilson

Author: Valerie Hough

Date: 11/23/2009



1. What information will be collected for the system (Ex. Name, Social Security Number, annual income, etc)?
Name, Social Security Number, Date-of-Birth, and address.
2. Why is this information being collected?
PII data is needed so that a unique borrower can be identified for former or current federal student aid recipients.
3. How will FSA use this information?
Information is needed to identify individuals that have received federal student aid
4. Will this information be shared with any other agency? If so, with which agency or agencies?
<p>The Department of Education may disclose information contained in a record in an individual's account under the routine uses listed in the Privacy Act System of Records notice without the consent of the individual if the disclosure is compatible with the purposes for which the record was collected. Specific disclosures include the following:</p> <ul style="list-style-type: none"> • Freedom of Information Act (FOIA) Advice Disclosure • Disclosure the Department of Justice • Contract Disclosure • Litigation and Alternative Dispute Resolution (ADR) Disclosure • Parties, counsels, representatives and witnesses • Administrative Disclosures • Federal and State agencies • Enforcement Disclosure • Employee Grievance, Complaint or Conduct Disclosure • Labor Organization Disclosure • Congressional Member Disclosure • Consumer reporting agency <p>These disclosures may be made on a case-by-case basis. If the Department has complied with the computer matching requirements of the Privacy Act, disclosure also may be made to another agency under a computer matching agreement.</p>



<p>There will be no sharing of information for purposes outside of the above disclosure requirements or for anything other than the primary purpose(s) of collecting the information. Any contractor responsible for the operations of the Financial Partners Data Mart (FPDM) is held to the privacy and security requirements of the Department of Education.</p>
<p>5. Describe the notice or opportunities for consent would be/ or are provided to individuals about what information is collected and how that information is shared with others organizations. (e.g., posted Privacy Notice)</p>
<p>A Privacy Act Statement Requirement is incorporated into the FPDM log on Privacy Policy articulating the specific authority for collecting personal information that will be maintained and retrieved by name or identifier from a Privacy Act system of records, the mandatory or voluntary nature of the information collected and the uses of the information. Before an individual can log into the FPDM system, they must read the Privacy Act Requirement statement and agree before the system will allow them access.</p>
<p>6. How will the information be secured? (An overview of security controls described in the system security plan (Technical Controls section) would be applicable to answer this question.)</p>
<p>The FPDM has been defined as a FIPS-199 Moderate system. The following security controls will be implemented to ensure the security of the information:</p> <p>Identification and Authentication, Access Control, Audit and Accountability; and System and Communications Protection. Further descriptions of these technical controls can be found in the FPDM System Security Plan.</p>
<p>7. Is a system of records being created or updated with the collection of this information? (A system of record is created when information can be retrieved from the system by the name of the individual or an identifying number, symbol or other identifying particular assigned to an individual. Also, in responding to this question a helpful reference may be to the system's System of Record organization step completed in the Definition phase of the Solution Lifecycle process.)</p>
<p>Yes, a system of records has been created with this collection of information. Users are provided notice of rights under the Privacy Act via links to the agency Privacy Act regulations (34 C.R.F. Part 5b.5) and to the Privacy Act system of</p>



records notice for the Financial Partners Data Mart.
8. List the web addresses (known or planned) that will have a Privacy Notice.
http://www.nslsfaf.ed.gov (Financial Aid Professional)
http://www.nsls.ed.gov/ (Students)
https://fp-mart.ed.gov (FPDM)