COALFIRE

Data Sheet

What is a CMS Privacy Impact Assessment?

Navigate CMS Privacy Compliance with Confidence and Expert Guidance

Privacy Impact Assessments (PIAs) are mandated by the E-Government Act of 2002 to enhance federal electronic government services. Specifically, Section 208 requires PIAs when a federal agency develops or acquires new technology that collects, maintains, or disseminates personally identifiable information.

Privacy Impact Assessment Introduction

A Privacy Impact Assessment (PIA) is a formal analysis that evaluates how an organization collects, uses, shares, and maintains personally identifiable information (PII). Some examples of PII include:

- **Identification numbers:** Social security number, passport number, driver's license number, taxpayer ID, patient ID, financial account, or credit card number.
- **Addresses:** Street or email address.
- **Personal characteristics:** Photos (especially of face), fingerprints, handwriting.
- **Names:** Full name, maiden name, mother's maiden name, alias.
- **Other information:** Location, events attended, status, sexual orientation, education, employment history, salary, job title, family, dependents, friends, usernames, or screen names.

The Purpose of a Privacy Impact Assessment (PIA)

PIAs demonstrate that system owners have intentionally included privacy protections for public information. OMB Memorandum 10-23 also requires the Centers for Medicare & Medicaid Services (CMS) to conduct a PIA for all Third-Party Websites and Applications (TPWAs), including analyzing social media sites and healthcare exchanges that CMS uses to engage with the public.

The Department of Health and Human Services (DHHS) requires a Privacy Impact Assessment (PIA) for all General Support Systems (GSSs) and Major Applications (MAs) under the Centers for Medicare & Medicaid Services (CMS). This ensures privacy protections are integrated throughout an IT system's lifecycle. The Office of Management and Budget (OMB) also mandates a PIA for all new IT funding requests. PIAs communicate information-handling practices to the public and demonstrate that system owners have implemented appropriate privacy protections.

Objectives of a Privacy Impact Assessment

A Privacy Impact Assessment (PIA) systematically identifies risks and potential effects related to collecting, maintaining, and disseminating Personally Identifiable Information (PII). A PIA aims to:

- Ensure the PII collected is relevant and necessary.
- Identify and address privacy risks and impacts.
- Confirm PII is collected, accessed, used, and shared only as needed and permitted.
- Verify PII is used for its intended purpose and is accurate and securely stored.
- Limit the retention of PII to only what is necessary.
- Comply with legal, regulatory, and policy requirements for privacy.
- Identify risks associated with PII and Protected Health Information (PHI)
- Recognize CMS information systems subject to the Privacy Act of 1974 to evaluate protections and alternative processes to mitigate potential privacy risks.

CMS requires documentation of Privacy and Security Audits for prospective primary and hybrid issuer upstream entities and applicable hybrid non-issuer upstream entities. The Privacy Impact Assessment (PIA) details the entity's controls for protecting Personally Identifiable Information (PII) and should be completed before the audit. While submitting the PIA to CMS is not mandatory, the agency may request it for review, including for audit purposes, as outlined in the Interconnection Security Agreement (ISA).

PIAs Must Be Completed In The Following Situations

- For all new systems that collect PII from 10 or more members of the general public, a PIA must be completed as part of the broader Authority to Operate (ATO) process.
- For every existing system that collects PII from 10 or more members of the general public, a PIA must be reviewed and re-approved once every three years. System/Business Owners and Information System Security Officers (ISSOs) must review and revise as necessary and submit PIAs for re-approval no later than three years from the last HHS approval date.
- For any existing system undergoing a significant change, an updated PIA is required.
- An existing system going through the ATO process may need to update its PIA paperwork if it's close to expiring; an ATO cannot be completed with an expired or incomplete PIA.

Our Approach

Coalfire leverages CMS templates and adapted the PASS (Pre-assessment, Analysis, Sampling and testing, Submission) methodology to ensure that the PIA assessment process follows a systematic approach covering documentation review, stakeholder engagement, control evaluation, and the development of actionable recommendations.

Deliverables

After the assessment, Coalfire provides clients with the following:

- **A report:** that documents the analysis of how PII is collected, used, shared, and maintained.
- **Identification of privacy risks:** An identification of any privacy risks associated with the system
- **Identification of options to address privacy risks:** A list of options for addressing any privacy risks identified in the PIA
- **Documentation of privacy protections:** Documentation of the privacy protections that have been incorporated into the system.

CMS - EDE Services

If you are new to CMS – EDE compliance or are working on an ATC, our experts can also help you with CME – EDE third-party audit support for the Business Audit, Privacy Assessment Planning (SAP), Privacy and Security Reports (SAR), and Privacy and Security Workbook (SAW) and POEM development. Our Advisory Services team can help develop your System Security and Privacy Plan (SSPP) and governance policies. Our knowledgeable consultants offer advisory services that can help you follow best practices and properly address CMS- EDE compliance requirements.

MARS-E Technical Testing

CMS effective with version 2.2 of the assessment template requires vulnerability and penetration tests for the in-scope system to be conducted during the SAR assessment window. Coalfire can leverage internal technical testing or provide services that can assist clients with meeting this requirement.

Copyright © 2025 Coalfire Systems, Inc. All rights reserved. Coalfire, the Coalfire Logo, CoalfireOne, the Coalfire|Talks Logo, the Hexagon Logo, Hexeon, Neuralys, RAMP/pak, RAMP/pak+, RAMPcon, the RAMPcon Logo, and ThreadFix are trademarks or registered trademarks of Coalfire Systems, Inc. or its affiliates in the United States and other countries. Other names may be trademarks of their respective owners.