



# CDC UNIFIED PROCESS PROCESS GUIDE



## PRIVACY IMPACT ASSESSMENT (PIA)

### Purpose of the Process Guide

CDC projects are required to comply with various CDC and Federal regulations, mandates, policies, processes, and standards. Information about these requirements is available from various websites and supporting documents. However, this information is often not presented from the perspective of the project team and their roles & responsibilities in complying with these requirements. CDC UP Process Guides provide that perspective.

CDC UP Process Guides help project teams comply with CDC and Federal requirements by:

1. Setting the requirements in the context of their purpose
2. Providing step-by-step instructions for completing the activities required for compliance
3. Illustrating potential integration points between processes
4. Presenting requirements in a concise, easy-to-understand, and consistent format
5. Making that presentation accessible to the CDC community via the CDC Unified Process website

The specific purpose of this Process Guide is to describe the **Privacy Impact Assessment (PIA)** process as it applies to project teams.

### Process Overview

CDC requires all HHS Privacy Impact Assessment (PIAs) to be processed in the early stages of the system lifecycle. PIA compliance and consistency with the C&A process will be ensured through the PIA processing activities.

The PIA process is used to determine what personally identifiable information (PII) is contained within an IT system, how that information is used, and how it is protected. It is important to complete the PIA process early in the planning phase of the project as results of the PIA could impact design. Systems with PII are subject to a set of requirements based on privacy laws, regulations, and guidance.

Conducting PIAs will allow CDC to identify which of its systems contain PII and which do not. For those systems containing PII, the PIA will serve as a platform to:

- Ensure information handling conforms to applicable legal, regulatory, and policy requirements regarding privacy.
- Determine the risks and effects of collecting, maintaining, and disseminating PII in an electronic information system.
- Examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

The PIA process involves completing the following two (2) sections of the HHS PIA Form:

1. **PIA Summary** – Captures what type of information is collected and stored by an IT system, why the information is collected and what it is used for. IT system information from the PIA Summary is rolled up and published by HHS for public view Information <http://www.hhs.gov/pia/cdc/>
2. **PIA Required Information** – Captures information needed to determine privacy impact.



# CDC UNIFIED PROCESS PROCESS GUIDE



## PRIVACY IMPACT ASSESSMENT (PIA)

The PIA is part of the Certification & Accreditation (C&A) process and must be repeated whenever an IT system changes in a way that may create or reduce new privacy risks. For example:

- **Conversions** – Converting paper based records to electronic systems
- **Anonymous to Non-Anonymous** – Functions applied to existing information collection change anonymous information in to IFF
- **Significant System Management Changes** – New use of an existing IT system, including application of new technologies, which may significantly change how IFF is managed in the IT system
- **Significant Merging** – Agencies adopt or alter business processes and government databases holding IFF are merged, centralized, matched with other databases or otherwise significant manipulated
- **New Public Access** – User-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an information system that is accessed by members of the public
- **Commercial Sources** – Agencies systematically incorporate into existing information systems databases of IFF that have been purchased or obtained from commercial or public sources (Note: Merely querying such databases on an ad hoc basis using existing technology does not trigger the PIA process)
- **New interagency Uses** – Agencies collaborate on shared functions involving significant new uses or exchanges of IFF, such as the cross-cutting E-government initiatives; in such cases, the lead agency should prepare the PIA.
- **Internal Flow or Collection** – New IFF is added to an information collection and increases risks to personal privacy (for example, health or financial information)
- **Alteration in Character of Data** – when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information)

### Process Attributes

This section provides a list of process attributes to help project teams better understand the requirements necessary to comply with this process and to determine when and how they may impact their project.

PROCESS ATTRIBUTE	DESCRIPTION
<b>Process Owner(s)</b>	Thomas P. Madden
<b>Process Criteria</b>	CDC requires all Privacy Impact Assessments (PIA) to be part of the C&A process.
<b>Timing of Process in Project Life Cycle</b>	Initiate the PIA process in the early stages (initiation phase) of the system lifecycle.
<b>Estimated Level of Effort</b>	It is estimated that conducting each PIA template takes two hours assuming that all information needed is readily accessible. If an IT system does not contain PII, it will take approximately 60 minutes to complete the process.
<b>Associated Costs</b>	No cost to the project except the estimated level of effort described above.
<b>Process Prerequisites</b>	An understanding of the data that will be collected and/or stored.
<b>Process Dependencies</b>	C&A documents <a href="http://intranet.cdc.gov/ociso/CandA/GetStarted.html">http://intranet.cdc.gov/ociso/CandA/GetStarted.html</a>
<b>Available Training</b>	<a href="http://intranet.hhs.gov/infosec/privacy.html">http://intranet.hhs.gov/infosec/privacy.html</a>
<b>Additional Information</b>	<a href="http://intranet.cdc.gov/ociso/privacy/privacy_management.html">http://intranet.cdc.gov/ociso/privacy/privacy_management.html</a> <a href="http://intranet.cdc.gov/ociso/CandA/CandAdocs/SPORT_%2006.1_%20HHS_Privacy_Impact_Assessment_Template.doc">http://intranet.cdc.gov/ociso/CandA/CandAdocs/SPORT_%2006.1_%20HHS_Privacy_Impact_Assessment_Template.doc</a>



# CDC UNIFIED PROCESS PROCESS GUIDE



## PRIVACY IMPACT ASSESSMENT (PIA)

### Contact List

This section provides a list of individuals and/or offices that are available to assist the project team in answering questions regarding the content of this Process Guide and related topics. The information is correct as of this publication. However, due to the ever-changing nature of our work environment it is possible some information may be out of date.

NATIONAL CENTER	ROLE	NAME
CDC Office of the Chief Operating Officer (OCIO)	Chief Information Officer	James D. Seligman
CDC Office of the Chief Information Officer (OCISO)	Chief Information Security Officer and Senior Official for Privacy	Thomas P. Madden
CDC Office of the Chief Information Officer (OCISO)	Compliance & Education (C&E) Project Manager	Felicia P. Kittles

### Key Terms

The CDC Unified Process Team maintains a comprehensive list of key terms and acronyms relevant to all Unified Process artifacts maintained on the CDC UP website. Follow the link below for definitions and acronyms related to this and other, documents.

<http://www2.cdc.gov/cdcup/library/other/help.htm>

### Activities Checklist

This section provides a list of steps outlining the activities associated with complying with this process. Due to the dynamic nature of the PIA process a website has been established to communicate the most current information regarding PIA requirements. This website also contains a list of the related templates that assist in completing PIA activities. <http://intranet.cdc.gov/ociso/privacy/PIA.html>

### Process Flowchart

This section provides a pictorial view of steps outlining the activities associated with complying with the PIA process and those responsible for those activities.



# CDC UNIFIED PROCESS PROCESS GUIDE



## PRIVACY IMPACT ASSESSMENT (PIA)

C&A-PIA Flowchart

