
Privacy Impact Assessment
for the

# Automation of Reports & Consolidation Orders System II

# (ARCOS-2)

## August 8, 2006

**Contact Point**
**Drug Enforcement Administration**
**Office of Diversion Control**
**202-307-1000**

**Reviewing Official**
**Jane C. Horvath**
**Chief Privacy Officer and Civil Liberties Officer**
**Department of Justice**
**(202) 514-0049**

# Introduction

ARCOS-2 supports the requirements of the Controlled Substances Act of 1970 to furnish an automated inventory and history of the transactions of legally manufactured pharmaceuticals. This information provides estimates of amounts of reportable substances used for medical and scientific needs within the U.S.; intelligence to investigators tracking the illegal diversion of these drugs; evidence to prosecutors in criminal diversion cases; and information to the United Nations on U.S. drug production.

# Section 1.0
# The System and the Information Collected and Stored within the System.

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

## 1.1 What information is to be collected?

The information collected is transactions of sales, purchases, and other activities affecting inventories of controlled substances.

## 1.2 From whom is the information collected?

The information collected is from drug manufacturers and wholesale distributors.

# Section 2.0
# The Purpose of the System and the Information Collected and Stored within the System.

The following questions are intended to delineate clearly the purpose for which information is collected in the system.

## 2.1 Why is the information being collected?

The data in ARCOS is used to track regulatory compliance in drug industry and detect abuse of legally manufactured pharmaceuticals that are diverted to the illegal market.

## 2.2 What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

CSA Reorganization Plan 192 and the Comprehensive Drug Abuse Prevention and Control Act of 1970 as amended. See 28 CFR 0.100

## 2.3 Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

Personally identifiable information of physicians, pharmacies, hospitals, teaching institutions, distributors and manufacturers are not included in the original submission of data, i.e., data being collected, however, names, addresses, and descriptions of drugs purchased are added during processing.

# Section 3.0
# Uses of the System and the Information.

The following questions are intended to clearly delineate the intended uses of the information in the system.

## 3.1 Describe all uses of the information.

The data in ARCOS is used to track regulatory compliance in the pharmaceutical drug industry and to detect abuse of legally manufactured pharmaceuticals that are diverted to illegal markets. This information provides estimates of amounts of reportable substances used for medical and scientific needs within the U.S.; intelligence to investigators tracking the illegal diversion of these drugs; evidence to prosecutors in criminal diversion cases; and information to the United Nations on U.S. drug production.

## 3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

Yes; the system does have rudimentary data mining capability to identify high quantity purchasers through standard statistical measurement tools; i.e., analysis of variance (ANOVA) techniques. The information identified from this capability includes a DEA Registration Number, Name, Address, Business Activity, i.e., pharmacy, hospital, physician, etc., and description of drugs purchased.

## 3.3 How will the information collected from individuals or derived from the system, including the system itself be checked for accuracy?

Import procedure is filled with edits that verify data coming in. Currently working on analysis and corrections to the Drug Data Dictionary file from information collected from pharmacies, and data files for data uploaded from the ARCOS system.

## 3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

Currently there are five years of transaction data available for querying online. The data prior to that is archived to tape and is available on a case by case basis. Data in the other supporting files, i.e., the Drug Dictionary File, the Transaction Error File, the Inventory file, the Participant File, and other table files are kept current and active until archived, since the system's inception in 1997.

## 3.5 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Only the Office of Diversion Control, Diversion Investigators, and a limited number of Agents, have access to ARCOS via approval from the Office of Security Programs.

## Section 4.0
## Internal Sharing and Disclosure of Information within the System.

The following questions are intended to define the scope of sharing both within the Department of Justice and with other recipients.

### 4.1 With which internal components of the Department is the information shared?

None.

### 4.2 For each recipient component or office, what information is shared and for what purpose?

N/A

### 4.3 How is the information transmitted or disclosed?

N/A

### 4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

N/A

# Section 5.0
# External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DOJ which includes foreign, Federal, state and local government, and the private sector.

## 5.1 With which external (non-DOJ) recipient(s) is the information shared?

Information is shared with other Federal agencies, state and local enforcement groups, medical and educational institutions.

## 5.2 What information is shared and for what purpose?

The information shared includes pharmaceutical trends/patterns and the controlled substance purchase histories of DEA Registrants. The purpose of sharing this information is to provide specific individuals with geographic hot spots, support civil and/or criminal cases, and assist in targeting drug diversion.

## 5.3 How is the information transmitted or disclosed?

Information is transmitted internally via email and disclosed to outside sources via CD, hardcopy, diskette, and email.

## 5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

Yes, if sensitive data is included.

## 5.5 What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

No training required.

## 5.6 Are there any provisions in place for auditing the recipients' use of the information?

Yes.

## 5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

Personally identifiable information of physicians, pharmacies, hospitals, teaching institutions, distributors and manufacturers are not included in the original submission of data, i.e., data being collected, however, names, addresses, and descriptions of drugs purchased are added during processing.

## Section 6.0
## Notice

The following questions are directed at notice to the individual of the scope of information collected, the opportunity to consent to uses of said information, and the opportunity to decline to provide information.

### 6.1 Was any form of notice provided to the individual prior to collection of 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 Notice.) If notice was not provided, why not?

No; not required.

### 6.2 Do individuals have an opportunity and/or right to decline to provide information?

No.

### 6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

No.

### 6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

N/A.

## Section 7.0
## Individual Access and Redress

The following questions concern an individual's ability to ensure the accuracy of the information collected about him/her.

### 7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

Individuals may not request information and amend their records pursuant to the Privacy Act, because this system is exempt. However, individuals may contact the agency representative in order to report abnormalities. This information is in the System of Record Notice (ARCOS/DADS) Justice / DEA 003.

### 7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

Not provided and not required.

### 7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

No.

### 7.4 Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

None.

# Section 8.0
# Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

## 8.1 Which user group(s) will have access to the system?

Diversion Investigators and Program Analysts in the field and at headquarters.

## 8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

Contractors maintain the system code and the data. See Appendix.

## 8.3 Does the system use "roles" to assign privileges to users of the system?

Yes.

## 8.4 What procedures are in place to determine which users may access the system and are they documented?

The user has to be granted access to the ARCOS-2 system through the Office of Security Programs.

## 8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Though Security Programs (SIP) and the Database and Web Management Unit (SISS).

## 8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

The ARCOS II system is setup to audit user sessions from the login to ARCOS II to logout. Audit data is downloaded to tapes and disk daily and is used by Security Programs to monitor user activity.

Each user is assigned an ARCOS II account that limits their access to designated files and resources. Users in ARCOS II are also assigned to classes that restrict their access to only those subsystems that have been authorized by their supervisor to use.

## 8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

Once a year security training.

## 8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

The date of the last C&A for ARCOS II was September 15, 2003.

## 8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Access to the system is available only to authorized users. Data requests to external organizations are either aggregate data without sensitive information or have the sensitive data redacted prior to disseminating the information. Therefore, the impact is minimal.

# Section 9.0
# Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

## 9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

Yes.

## 9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

The Office of Security Programs controls access to ARCOS information. Protocols exist for data integrity and security.

## 9.3 What design choices were made to enhance privacy?

Password protected systems.

## Responsible Officials

_____/s/_____<<Signature>> _____<<Date>>

Richard W. Sanders
Assistant Administrator
Chief Privacy Officer
Drug Enforcement Administration

_____/s/_____<<Signature>> _____<<Date>>

Wendy H. Goggin
Chief Counsel
Chief Privacy Official
Drug Enforcement Administration

## Approval Signature Page

_____/s/_____<<Signature>> _____<<Date>>

Jane Horvath
Chief Privacy and Civil Liberties Officer
Department of Justice