

# 2010 Data Protection Seminar

TMA Privacy Office



## Understanding the Privacy Impact Assessment



HEALTH AFFAIRS



TRICARE  
Management Activity

## Understanding the Privacy Impact Assessment

# Purpose

---

Provide a high-level overview of Privacy Impact Assessments (PIAs), the TRICARE Management Activity (TMA) PIA process, the DoD PIA template (DD Form 2930), and responsibilities regarding completion of PIAs



HEALTH AFFAIRS



## Understanding the Privacy Impact Assessment

# Objectives

---

- Upon completion of this presentation, you should be able to:
  - Explain PIAs and how they help safeguard personally identifiable information (PII) and protected health information (PHI)
  - Recognize definitions of basic PIA terms
  - Explain the DoD PIA policy
  - Explain the DoD PIA template
  - Explain the PIA process
  - Discuss PIA after-action items



## Understanding the Privacy Impact Assessment

# What is a PIA?

---

- A PIA is an analysis of how PII is safeguarded in an information technology (IT) system
- A PIA can be performed at any time during a system's lifecycle
  - PIAs can be performed on a “conceptual system”
  - PIAs should be started in the earliest stages of the system lifecycle
  - PIAs are performed on legacy systems



## Understanding the Privacy Impact Assessment

# What is a PIA? (continued)

---

- PIAs are conducted to:
  - Ensure that systems conform to privacy requirements
  - Assess risks
  - Mitigate potential risks
- Four main goals of a PIA are:
  - Verification and validation
  - Accountability
  - Consistency
  - Remediation



## Understanding the Privacy Impact Assessment

# What is a PIA? (continued)

---

- A PIA must be a standalone document
- A PIA must be consistent with a system's security documentation
- A PIA must be consistent with applicable System of Records Notices (SORNs)
- A PIA is one way that federal agencies inform the public on uses of their PII



HEALTH AFFAIRS



## Understanding the Privacy Impact Assessment

# PIA Terminology

---

- PII: Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual



HEALTH AFFAIRS

Source: Privacy Impact Assessment DDForm 2930, Appendix



## Understanding the Privacy Impact Assessment

# PIA Terminology (continued)

---

- PHI: Individually identifiable health information. Information that is a subset of health information, including demographic information collected from an individual, and:
  - Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
  - Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
    - That identifies the individual; or
    - With respect to which there is a reasonable basis to believe the information can be used to identify the individual



HEALTH AFFAIRS

Source: DoD 6025.18-R, DoD Health Information Privacy Regulation



## Understanding the Privacy Impact Assessment

# PIA Terminology (continued)

---

- Electronic collection: Any collection of information enabled by IT
- DoD information system: Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system applications, enclaves, outsourced IT-based processes, and platform IT interconnections
- Federal personnel: Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits)



HEALTH AFFAIRS

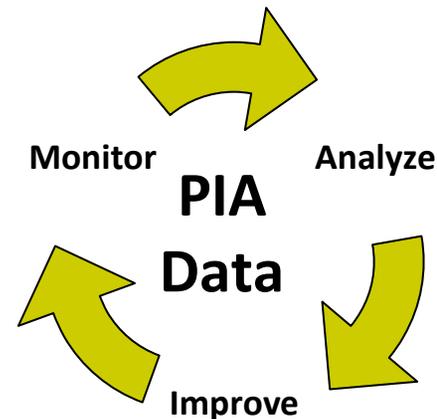
Source: Privacy Impact Assessment DDForm 2930, Appendix



## Understanding the Privacy Impact Assessment

# Importance of Conducting PIAs

- DoD takes its responsibility seriously when safeguarding PII/PHI and preventing its theft, loss, or compromise
- DoD addresses privacy and security challenges through many initiatives including PIAs and ensuring that DoD employees are aware of their privacy responsibilities



## Understanding the Privacy Impact Assessment

# Importance of Conducting PIAs (continued)

---

- Completion of the PIA is a part of the DoD Information Assurance Certification and Accreditation Process (DIACAP)
  - Failure to complete a PIA may result in delays to your system's certification



HEALTH AFFAIRS



## Understanding the Privacy Impact Assessment

# Importance of Conducting PIAs – Federal and DoD

---

- E-Government Act of 2002 § 208
- Federal Information Security Management Act (FISMA) of 2002
- Office of Management and Budget (OMB)
  - Memorandum (M) 03-22: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
  - Circular A-11: Preparation, Submission, and Execution of the Budget, August 2009 (capital planning process/Exhibit 300s)
- DoD Instruction 5400.16 “DoD Privacy Impact Assessment (PIA) Guidance”



## Understanding the Privacy Impact Assessment

# PIA Requirements

---

- Federal agency PIA requirements
  - Section 208 of the E-Government Act of 2002 requires all agencies to conduct PIAs for all new or substantially changed information systems that collect, maintain, or disseminate PII on the public
- DoD PIA requirements
  - DoD Instruction 5400.16 expands the coverage to include federal personnel, contractors, and foreign nationals employed at United States military facilities internationally



HEALTH AFFAIRS



## Understanding the Privacy Impact Assessment

# Highlights of DoDI 5400.16

---

- Formalizes E-Government Act PIA requirement in DoD for greater visibility and clarity
- Enhances responsibilities and accountability
  - DoD Program Manager (PM) or designee starts the assessment
  - Requires coordination with PM, Information Assurance, and Component Privacy
  - Expands signature requirements



## Understanding the Privacy Impact Assessment

# Highlights of DoDI 5400.16 (continued)

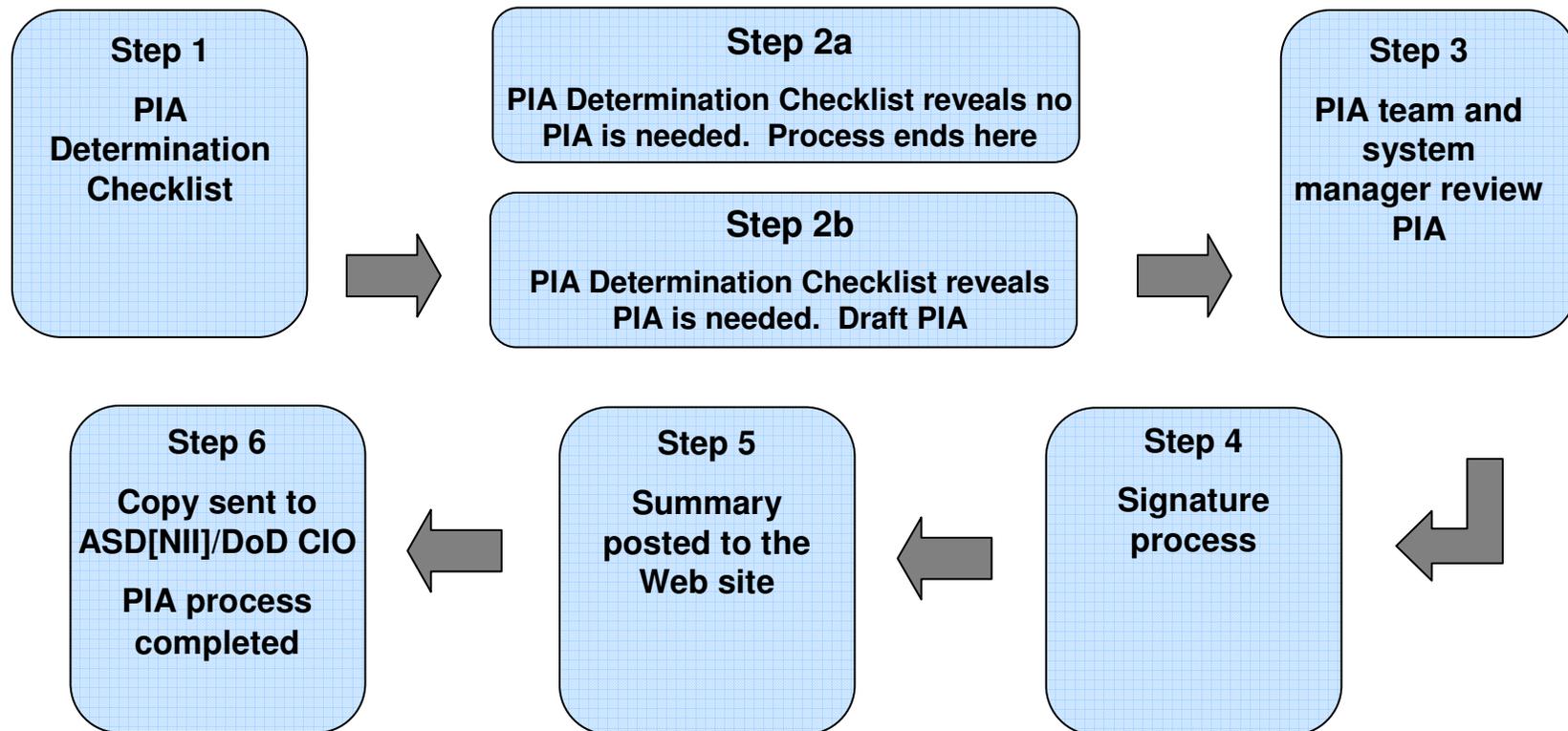
---

- Better coordination with other processes
  - Privacy Act SORNs
  - Information Collection
  - Certification and Accreditation (C&A)
  - Budget
- Establishes review cycle
- Structures privacy risk identification and assessment with DoD PIA Form (DD 2930)



# Understanding the Privacy Impact Assessment

## Overview of the PIA Process



# Understanding the Privacy Impact Assessment

## Overview of the PIA Process (continued)

### PIA Determination Checklist

- The PIA Determination Checklist helps determine if a PIA is required
- This is a TMA Privacy Office assessment tool
- Prior to starting a PIA, the program manager completes the Checklist and submits it to the TMA Privacy Office
- If a PIA is not needed, the process stops here
- The Checklist is kept on file for future reference on how the determination was made

**TMA Privacy Office  
Privacy Impact Assessment Determination Checklist**

Information System/Electronic Collection Name: _____	
Program Office: _____	Government POC: _____
POC: _____	Title: _____
Title: _____	Phone: _____
Phone: _____	Email: _____
Email: _____	

1. Does the system collect, maintain, and/or disseminate PII/PHI?  YES  NO
2. Is a system description attached to this document?  YES  NO
3. Has a PIA Determination Checklist been previously submitted for this system?  YES  NO  
If yes, date submitted: \_\_\_\_\_
4. Has a full PIA been previously submitted for this system?  YES  NO  
If yes, date submitted: \_\_\_\_\_  
\*If yes, have there been changes to the system?  YES  NO
5. Is this system covered by a DUA, DMA or other Data Agreement?  YES  NO  
If yes, please provide the DUA Number: \_\_\_\_\_

System Manager: (print) _____	Date: _____
System Manager: (signature) _____	
PIA Required: <input type="checkbox"/> YES <input type="checkbox"/> NO	Privacy Officer: (signature): _____
	Date: _____

\*Provide details in system description.

TMA Privacy Office Comments:



# Understanding the Privacy Impact Assessment

## Overview of the PIA Process (continued)

### PIA System Information

- Defense Health Program (DHP)-funded systems are identified using numbers and names that have been established for purposes other than the PIA submission, including:
  - IT investment unique identifier
  - Budget system identification number (IT Registry)
  - System identification number (IT Registry)

### PRIVACY IMPACT ASSESSMENT (PIA)

For the

Enter DoD Information System/Electronic Collection Name

Enter DoD Component Name

#### SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

- (1) Yes, from members of the general public.
- (2) Yes, from Federal personnel\* and/or Federal contractors.
- (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- (4) No

\* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

DD FORM 2930 NOV 2008

Page 1 of 15



HEALTH AFFAIRS



# Understanding the Privacy Impact Assessment

## Overview of the PIA Process (continued)

### PIA System Description

- Key information includes:
  - Issued by Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Office (ASD[NII]/DoD CIO)
  - System description: Purpose, boundaries, etc.
  - System development life cycle C&A status
  - Circular A-11 capital planning exhibits
  - PII maintained in the system
  - Subjects of PII

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

Within the DoD Component.

Specify.

Other DoD Components.

Specify.

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

Contractor (Enter name and describe the language in the contract that safeguards PII.)

Specify.

Other (e.g., commercial providers, colleges).

Specify.

DD FORM 2930 NOV 2008

Page 4 of 15



HEALTH AFFAIRS



# Understanding the Privacy Impact Assessment

## Overview of the PIA Process (continued)

### PIA Information Sharing

- Key points include:
  - Privacy Act of 1974 compliance
  - Collecting PII from sources other than directly from individuals (databases, Web sites, etc.)
  - Populating PII for other resources (databases, Web sites, etc.)
  - Sharing or disclosing PII outside the service
  - Computer Matching and Privacy Protection Act
  - Individual choice and notification

i. Do individuals have the opportunity to object to the collection of their PII?

Yes  No

(1) If "Yes," describe method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

Yes  No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

FD FORM 2930 NOV 2008

Page 5 of 15



HEALTH AFFAIRS



# Understanding the Privacy Impact Assessment

## Overview of the PIA Process (continued)

### PIA Security Controls

- Key resources include:
  - Security control assessments
  - Contingency plans
  - System and data backup plans
  - Password controls
  - Incident response plans
  - Physical controls
  - Controls on the use of mobile computing devices, removable storage media, remote access

### SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply below.

- |   |   |   |
|---|---|---|
| <input type="checkbox"/> Name                           | <input type="checkbox"/> Other Names Used       | <input type="checkbox"/> Social Security Number (SSN) |
| <input type="checkbox"/> Truncated SSN                  | <input type="checkbox"/> Driver's License       | <input type="checkbox"/> Other ID Number              |
| <input type="checkbox"/> Citizenship                    | <input type="checkbox"/> Legal Status           | <input type="checkbox"/> Gender                       |
| <input type="checkbox"/> Race/Ethnicity                 | <input type="checkbox"/> Birth Date             | <input type="checkbox"/> Place of Birth               |
| <input type="checkbox"/> Personal Cell Telephone Number | <input type="checkbox"/> Home Telephone Number  | <input type="checkbox"/> Personal Email Address       |
| <input type="checkbox"/> Mailing/Home Address           | <input type="checkbox"/> Religious Preference   | <input type="checkbox"/> Security Clearance           |
| <input type="checkbox"/> Mother's Maiden Name           | <input type="checkbox"/> Mother's Middle Name   | <input type="checkbox"/> Spouse Information           |
| <input type="checkbox"/> Marital Status                 | <input type="checkbox"/> Biometrics             | <input type="checkbox"/> Child Information            |
| <input type="checkbox"/> Financial Information          | <input type="checkbox"/> Medical Information    | <input type="checkbox"/> Disability Information       |
| <input type="checkbox"/> Law Enforcement Information    | <input type="checkbox"/> Employment Information | <input type="checkbox"/> Military Records             |
| <input type="checkbox"/> Emergency Contact              | <input type="checkbox"/> Education Information  | <input type="checkbox"/> Other                        |

If "Other," specify or explain any PII grouping selected.

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

Describe here.



# Understanding the Privacy Impact Assessment

## Overview of the PIA Process (continued)

### PIA Summary Review

- Signatures may include:
  - Preparing Official (a government employee)
  - Senior Information Assurance Official
  - Reviewing Officials
  - Chief Privacy Office (CPO)
  - Chief Information Office (CIO)

### SECTION 4: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

Program Manager or Designee Signature

Name:

Title:

Organization:

Work Telephone Number:

DSN:

Email Address:

Date of Review:

Other Official Signature  
(to be used at Component discretion)

Name:

Title:

Organization:

Work Telephone Number:

DSN:

Email Address:

Date of Review:



## Understanding the Privacy Impact Assessment

# Overview of the PIA Process (continued)

---

- After-action items
  - File sent to ASD[NII]/DoD CIO
  - Copy kept in TMA Privacy Office
  - PIAs (sections one and two) are posted to the TMA Privacy Office Web site
- Create a plan of action to mitigate identified risks
- Keep TMA Privacy Office informed: [PIAmail@tma.osd.mil](mailto:PIAmail@tma.osd.mil)
- PIA review in conjunction with C&A or three years from date of approval, whichever comes first



## Understanding the Privacy Impact Assessment

# Summary

---

- You should now be able to:
  - Explain PIAs and how they help safeguard PII and PHI
  - Recognize definitions of basic PIA terms
  - Explain the DoD PIA policy
  - Explain the DoD PIA template
  - Explain the PIA process
  - Discuss PIA after-action items



## Understanding the Privacy Impact Assessment

# Resources

---

- E-Government Act of 2002 § 208, December 17, 2002
- Office of Management and Budget Memorandum 03-22: “OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002”, September 26, 2003
- Office of Management and Budget Circular A-11: “Preparation, Submission, and Execution of the Budget”, August 7, 2009



HEALTH AFFAIRS



## Understanding the Privacy Impact Assessment

### **Resources** (continued)

---

- DoD Instruction 5400.16 “DoD Privacy Impact Assessment (PIA) Guidance”, February 12, 2009
- DoD PIA Template – DD Form 2930
- E-mail [PIAmail@tma.osd.mil](mailto:PIAmail@tma.osd.mil) for subject matter questions
- For more information on PIAs go to:  
<http://www.tricare.mil/tma/privacy/pias.aspx>
- To subscribe to the TMA Privacy Office E-News, go to:  
<http://www.tricare.mil/tma/privacy/maillinglist.aspx>

