

2010 Data Protection Seminar

TMA Privacy Office



Privacy Act Implications: Data Collections and Systems of Records



HEALTH AFFAIRS



TRICARE

TRICARE
Management Activity

Privacy Act Implications: Data Collections and Systems of Records

Purpose

Provide a high-level overview of Privacy Act requirements as implemented within the DoD regarding collections of data from individuals and maintenance, use, and disclosure of that data in DoD owned and operated systems of records



HEALTH AFFAIRS



Privacy Act Implications: Data Collections and Systems of Records

Objectives

- Upon completion of this presentation, you should be able to:
 - Describe how the Privacy Act is implemented within and applies to DoD Components for the direct solicitation and collection of records of personally identifiable information (PII), including protected health information (PHI)
 - Identify the implications of the Privacy Act with respect to operation and maintenance of systems of records by or on behalf of DoD Components
 - Explain how DoD Components can be held accountable for misuse or mishandling of PII and PHI, including unauthorized or impermissible disclosures of data



Privacy Act Implications: Data Collections and Systems of Records

DoD Privacy Program

- Implementation of the Privacy Act of 1974 within the DoD by DoD 5400.11-R, “Department of Defense Privacy Program”
- Personal privacy of an individual shall be protected all times
- Direct solicitation and collection of data from individuals, must be “relevant” and “no more than the minimum necessary to accomplish a lawful purpose”



HEALTH AFFAIRS



Privacy Act Implications: Data Collections and Systems of Records

Privacy Act Statement Notices & Privacy Advisories

- The Privacy Act requires “notice” to individuals “at or before” the point of solicitation and collection of their PII
- There are two different forms of notice to individuals:
 - Privacy Act Statements: Required for **collection** of PII from individuals that will be saved in a system of records
 - Notice of Privacy Practices (NoPP) is provided to individuals the collection to describe DoD use and disclosure
 - Privacy Advisory: Required for **use** of PII (but not saved in a system of records)



Privacy Act Implications: Data Collections and Systems of Records

Privacy Act Statement Notices & Privacy Advisories

Privacy Act Statements: For “collections” of PII

- Purpose
- Authorities
- Routine uses
- Disclosures

Privacy Advisories: For “use” of PII

- A natural language description that puts the reader in a “privacy frame of mind”
- Privacy Act
- No collection, only use



Privacy Act Implications: Data Collections and Systems of Records

Systems of Records

- A system of records is a group of records under the control of a DoD Component from which personal information is retrieved by the individual's name or by some other personal identifier assigned to the individual
 - The “ability to retrieve” is not enough – actual retrieval is required
 - Retrieval by “personal identifier” – that which is linked or linkable to an individual



HEALTH AFFAIRS



Systems of Records Notices

- Advance public notice must be given before DoD begins to collect personal information for a system of records
- A System of Records Notice (SORN) must be published in the *Federal Register* before a system can lawfully operate
 - “Dummy” vs. “Live” – there is no exception for testing
- A SORN explains the existence and character of any system of records to be established (or revised)



Anatomy of a SORN

- SORNs are a blueprint of system and provide useful information such as:
 - System name, authorities, categories of records, purpose, routine uses, record sources, retrievability and safeguards



Privacy Act Implications: Data Collections and Systems of Records

The SORN Process

- SORN reviews begin in the TRICARE Management Activity (TMA) Privacy Office where there is intake, discussion and analysis, and preparation of a preliminary draft
- SORNs are then submitted up to the Office of the Secretary of Defense (OSD)/Joint Staff (JS) Privacy Office Washington Headquarters Services (WHS) for comment
- SORNs are finally sent to Defense Privacy Office (now Defense Privacy and Civil Liberties Office) for final approval and publication for:
 - Public comment
 - Final publication



Privacy Act Implications: Data Collections and Systems of Records

SORNs – Routine Uses versus Purpose

- Routine use disclosures: Uses and disclosures made from systems of records “outside” of the DoD (and without individual consent) are permitted if one of the DoD “routine uses” applies
 - Note: “Blanket Routine Uses”
- Purpose: By contrast “internal uses” are those constituting the *purpose* of the information collection



HEALTH AFFAIRS



Privacy Act Implications: Data Collections and Systems of Records

SORNs – Protected Health Information

- Under routine uses, there is room to discuss how PHI is maintained, used, and disclosed when present in a system
 - Note 1: Standard language citing the HIPAA Privacy Rule (45 C.F.R. Parts 160 and 164)
 - Note 2: Standard language citing 42 U.S.C. 290-dd regarding “confidentiality of records”



HEALTH AFFAIRS



Privacy Act Implications: Data Collections and Systems of Records

SORNs – Safeguards

- Physical, administrative, and technical
 - Common Access Card enabled
 - Role-based access controls
 - Training
 - Audit logs



Privacy Act Implications: Data Collections and Systems of Records

SORNs – Disclosures

- A DoD component is prohibited from disclosing records pertaining to an individual from a system of records except with the consent of the individual or pursuant to a published “routine use”
 - Improper disclosures trigger breach notification and response rules. If individually identifiable health information is disclosed, additional rules may apply. These rules are explained in a separate presentation on breach notification and response
- Records of disclosures must be maintained, because individuals are entitled by right to obtain an accounting of such disclosure



Privacy Act Implications: Data Collections and Systems of Records

SORNs – TMA Privacy Office

- Coordinate all SORN submissions for Health Affairs (HA) and TMA
- Serve as the point of contact as for all new, altered, amended, changed, or deleted systems as appropriate
- Coordinate with program/system managers to review policies, practices that apply to new or existing systems
- Maintain the OSD specific inventory of SORNs for TMA



HEALTH AFFAIRS



Privacy Act Implications: Data Collections and Systems of Records

Penalties for Privacy Act Non-Compliance

- Non-compliance with the Privacy Act carries misdemeanor criminal penalties and fines of up to \$5000 for
 - Soliciting or collecting individual data under false pretenses
 - Unauthorized disclosure without written permission or consent
 - Maintaining or collecting data for a system of records without meeting public notice requirements
- There are also substantial civil penalties including awards for actual damages, payment of reasonable attorney fees, and removal from employment



Privacy Act Implications: Data Collections and Systems of Records

Summary

- You should now be able to:
 - Describe how the Privacy Act is implemented within and applies to DoD Components for the direct solicitation and collection of records of PII, including PHI
 - Identify the implications of the Privacy Act with respect to operation and maintenance of systems of records by or on behalf of DoD Components
 - Explain how DoD Components can be held accountable for misuse or mishandling of PII and PHI, including unauthorized or impermissible disclosures of data



Privacy Act Implications: Data Collections and Systems of Records

Resources

- The Privacy Act of 1974, as amended (5 U.S.C § 552a)
- OMB Memorandum 99-05, “Instructions on complying with President’s Memorandum of May 14, 1998, ‘Privacy and Personal Information in Federal Records’”, January 7, 1999, Attachment B
- OMB Circular A-130, “Management of Federal Information Resources”, November 28, 2000



Privacy Act Implications: Data Collections and Systems of Records

Resources (continued)

- OSD Administrative Instruction No. 81, “OSD/Joint Staff (JS) Privacy Program”, November 20, 2009
- E-mail SORmail@tma.osd.mil for subject matter questions related to SORN
- E-mail PrivacyOfficerMail@tma.osd.mil for subject matter questions related to the Privacy Act
- To subscribe to the TMA Privacy Office E-News, go to: <http://www.tricare.mil/tma/privacy/maillinglist.aspx>

