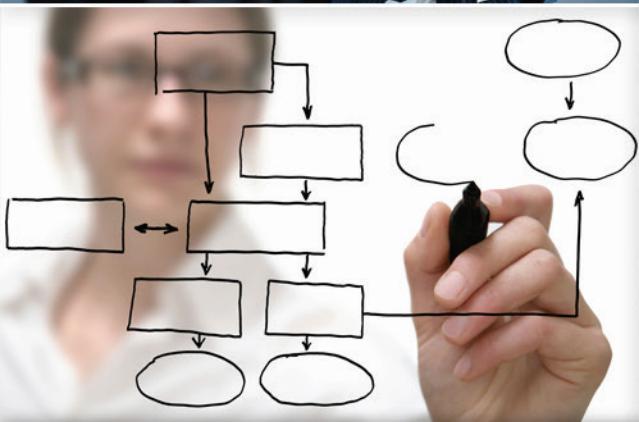


TMA PRIVACY AND CIVIL LIBERTIES OFFICE

2012 HEALTH INFORMATION PRIVACY & SECURITY TRAINING



Federal Privacy Overview

THE POWER OF TEAM WORK

Committed to Protecting Beneficiary Data

Federal Privacy Overview

Purpose

The purpose of this presentation is to provide a high level overview of Privacy Act of 1974, 5 United States Code (U.S.C.) 552a (Privacy Act) requirements on systems of records, System of Record Notices (SORNs), and Privacy Impact Assessments (PIA), and to identify basic compliance responsibilities of contractors under the Privacy Act.



Objectives

- Upon completion of this presentation, you should be able to:
 - Discuss how the Privacy Act is implemented within the Military Health System (MHS) and its impact on those who solicit and collect records of personally identifiable information (PII) on behalf of the TRICARE Management Activity (TMA)
 - Describe how DoD employees and contractors can be held accountable for misuse or mishandling of PII
 - Identify other federal law and regulations that define and establish rights and protections when federal agencies collect PII



What is PII?

- PII refers to personally identifiable information
- Office of Management and Budget (OMB) M-06-19 defines PII as:
 - 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 (SSN), 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



Federal Privacy Overview

Examples of PII



Unique identifiers (SSN, Tribal Enrollment Number, etc.)



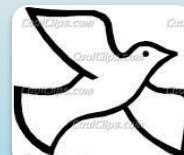
Personal contact information (home address, home phone number, personal e-mail, etc.)



Medical information



Financial information



Family information

Mother's maiden name, race, ethnicity, national origin

Beliefs/memberships when non-work related



Biometric data (fingerprints, eye scan, etc.)



Why Is it Important to Protect PII?

- It is legally required, and there are consequences for TMA, its contractors, and workforce members for non-compliance
- Individuals could have their identities stolen
- Individuals could experience embarrassment
- TMA could experience lawsuits, loss of public trust, and costly remediation efforts
- Individuals responsible for breaches could be subject to lawsuits, fines, and disciplinary action



Why Does TMA Collect PII?

- TMA and MHS is the largest integrated healthcare delivery system in the world, and it must collect PII from
 - Active duty, Reserve, and National Guard members of the Armed Forces
 - Retirees
 - Spouses and dependents
- TMA and MHS need PII to provide and/or pay for medical services for over 9.5 million beneficiaries
- TMA also collects PII to hire, pay, train, evaluate, and retire employees



Federal Privacy Overview

Privacy Framework

- Privacy Act of 1974 <http://www.justice.gov/opcl/privstat.htm>
- E-Government Act of 2002 <http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.2458.ENR:>
- Federal Information Security Management Act (FISMA)
<http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>
- Freedom of Information Act, as amended (FOIA)
<http://www.justice.gov/oip/amended-foia-redlined-2010.pdf>
- Paperwork Reduction Act <http://www.archives.gov/federal-register/laws/paperwork-reduction/>
- Clinger-Cohen
http://www.cio.gov/Documents/it_management_reform_act_feb_1996.html



Regulations and Guidance

- DoDD 5400.11, DoD Privacy Act Program
- DoD 5400.11-R, DoD Privacy Program
- OMB Guidance – also incorporates National Institute of Standards and Technology (NIST) requirements
- Guidance and instructions issued by the Defense Privacy and Civil Liberties Office
- TMA guidance
 - Administrative Instructions
 - TRICARE Operations Manual chapters
 - TMA policies and procedures



Privacy Act in Concert with HIPAA

- This presentation focuses on the statutory and regulatory framework application to PII
- TMA and the MHS must also be concerned with “protected health information” or PHI under HIPAA, as implemented within DoD by the DoD Health Information Regulation (DoD 6025.18-R)
- When deciding whether a particular PHI use and disclosure is permitted and/or subject to conditions, follow the provisions of whichever application rule is more restrictive



The Privacy Act of 1974

- Applies to federal agencies and incorporates the Fair Information Practices Principles:
 - Openness
 - Individual participation
 - Scope limitation on collection
 - Data quality
 - Finality of purpose for collecting
 - Security
 - Accountability



Privacy Act Policy Objectives

- To ***restrict disclosure*** of records contained in a system of records maintained by executive agencies
- To grant individuals increased ***rights of access*** to agency records maintained on themselves
- To grant individuals the ***right to seek amendment*** of agency records that are not accurate, relevant, timely, or complete
- To enact the above mentioned ***code of fair information practices***



Applicability of the Privacy Act

- Paper records
- Electronic records
- Databases
- Intra- and inter-agency data sharing
- Data warehouses
- Web sites and portals
- New technology (e.g., geographic information system, wireless, social media, cloud computing)



What Is a System of Records?

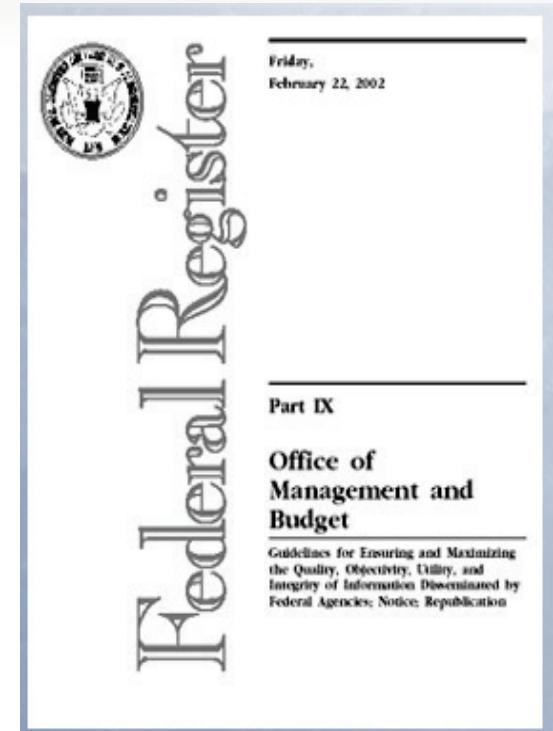
- A Privacy Act system of records is a group of records about individuals maintained by an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual, such as employee identification number
- The maintenance of a system of records requires a published SORN



Federal Privacy Overview

Keeping SORNs Current

- Whenever a new SORN is written, it must be published in the Federal Register. In addition, OMB and Congress must receive notice of the SORN prior to its publication
- A published SORN requires revision whenever there is even a minor change, such as a new system location or system manager. In addition to publishing the revised SORN in the Federal Register, whenever the change is significant, OMB and Congress must also be notified. Such notification is not necessary when the revision is minor



SORN Contents

- SORN contents are set by the National Archives and Records Administration for Federal Register Publication of Notices, and major components include:
 - System name, location, system manager
 - Main purpose(s) of the system of records
 - Categories of individuals and data collected
 - Routine uses – with whom privacy information may be shared outside the agency
 - Safeguards to the data – administrative, physical, and technical
 - How records are handled and disposed of
 - How records may be accessed or corrected by individuals



Sharing Privacy Information

- WITHIN DoD, privacy information maintained in Privacy Act systems of records may be shared with authorized employees for legitimate DoD business purposes
- OUTSIDE of DoD, privacy information may be shared in only these three ways:
 - With individual's informed, written consent
 - In accordance with ROUTINE USES in the SORN
 - Under one of the 12 exceptions of the Privacy Act



Other Privacy Act Provisions

- A Privacy Act Statement must be provided whenever PII is collected directly from an individual [5 U.S.C. 552a(e)(3)]
 - Any collection or form (paper, an electronic form, or Web) must show the purpose, routine uses, with whom the information will be shared, the legal authority for the collection, whether providing the information is voluntary, and any consequences of not providing the information
 - Applies whether collecting from public or workforce members
 - Can be either on the form, in a separate handout, or read to the individual



Privacy: Contractors and Their Workforce

- The Privacy Act requires:
 - When a contract provides for the operation by or on behalf of the DoD (or TMA) a system of records to accomplish an agency function, DoD shall cause the requirements of the Privacy Act to be applied to such system
 - Contracts must contain Federal Acquisition Regulation (FAR) Privacy Clauses 55.224-1 (Privacy Act Notification) and 52.224-2 (Privacy Act)
 - DoD 5400.11-R, the DoD Privacy Program, is applicable to contractors under DoD FAR 224.103
- Result: Contractors fulfilling agency functions (and their workforce members) have the same Privacy Act obligations as federal employees, including privacy training, care in handling, maintaining confidentiality of the PII, etc.



12 Exceptions to Non-Disclosure Requirement

- Agencies shall not disclose records contained in a system of records unless pursuant to individual written consent or one of the 12 exceptions below [5 U.S.C. 552a(b)]:
 1. To those ***officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;***
 2. Required ***under section 552 [FOIA]***
 3. For a ***routine use*** [SORN]
 4. To the ***Bureau of the Census*** for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13



12 Exceptions to Non-Disclosure Requirement

- 12 exceptions (continued):
 5. To a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a ***statistical research or reporting record***, and the record is to be transferred in a form that is not individually identifiable
 6. To the ***National Archives and Records Administration*** as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value



12 Exceptions to Non-Disclosure Requirement

- 12 exceptions (continued):

7. To another agency or to an instrumentality of any ***governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity*** if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought
8. To a person pursuant to a showing of ***compelling circumstances affecting the health or safety of an individual*** if upon such disclosure notification is transmitted to the last known address of such individual



12 Exceptions to Non-Disclosure Requirement

- 12 exceptions (continued):
 9. To ***either House of Congress***, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee
 10. To the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the ***Government Accountability Office***
 11. Pursuant to the ***order of a court of competent jurisdiction***
 12. To a ***consumer reporting agency*** in accordance with title [31](#)



Privacy Act Penalties

- Criminal penalties include a misdemeanor and fine up to \$5,000 for:
 - Knowingly maintaining a system of records without publishing the required SORN
 - Knowingly disclosing privacy information from a Privacy Act system of records outside the scope of an allowable purpose
 - Attempting to acquire privacy information under false pretenses
- Civil actions may also be brought by individuals against the agency when a Privacy Act violation occurs that harms the individual



Federal Privacy Overview

E-Government Act of 2002

- What are the major privacy requirements?
 - Develop PIA for electronic systems
 - Post privacy policies on agency Web sites
 - Implement Platform for Privacy Preferences Project (P3P) (machine-readable) privacy policies on agency Web sites



PIAs

- OMB M-03-22 defines a PIA as an analysis of how information is handled:
 - To ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy
 - To determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system
 - To examine and evaluate protections



Federal Privacy Overview

Main PIA Contents

- Identifies system, system manager
- OMB identifier, if applicable (relates to OMB A-11 unique ID code for the system as an investment)
- Identifies purposes of system
- Identifies data elements, and sources of data
- Discusses steps taken to ensure relevance, timeliness, accuracy, and completeness of data
- Identifies who has access to the data
- Identifies how data is protected (administrative, physical, and technical safeguards)
- Identifies statutory authority for system
- Identifies associated records schedule
- Identifies associated SORN if applicable



FISMA of 2002

- This is Title III of the E-Government Act of 2002
- Requires agency privacy reporting by Chief Information Officers, Senior Agency Officials for Privacy, and Inspectors General who conduct annual reviews of the agency's information security program, including privacy requirements, and report results to OMB
- The first stated purpose within FISMA is: "provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets [(§ 3541)]"
- Mandates security awareness training for employees
- Incorporates NIST requirements for agency information technology systems



Federal Privacy Overview

FOIA

- Protects privacy information. The FOIA requires redaction (removal and non-disclosure) of privacy information requested by a third party under exemptions 6 (general) and 7(C) (law enforcement records)
- Your TMA FOIA staff administers Privacy Act requests, in which the subject of the information (or their agent) is the requester. Individual requesters are normally entitled to their own information without redaction, unless the system is an exempt system, such as a law enforcement system



Paperwork Reduction Act of 1995

- Applies to any structured collection of information conducted by an agency from any non-federal source, if there are 10 or more instances in which an individual or organization provides information within any given year
- Requires any SORN and/or PIA requirements that may be associated with an information collection be fulfilled, including adequate protection of privacy information, before OMB approval, and that any forms used to collect information have the required Privacy Act Statement
- Requires that any form (whether paper or electronic) collecting privacy information contain not only the aforementioned Privacy Act Statement, but also a Paperwork Reduction Act Statement addressing the burden of the information collection



OMB Oversight and Guidance

- OMB is the lead authority for privacy compliance for executive agencies, and issues privacy guidance
- OMB requires quarterly and annual reporting on privacy related metrics and compliance through FISMA reporting such as how many of our SORNs and PIAs are completed, and how are we doing on reducing unnecessary use of SSN. This explains why you may get periodic data calls on such issues



DoD Privacy Regulations

- DoD Directive 5400.11 requires DoD components (such as TMA and DoD contractors operating a system of records on behalf of a DoD component) to protect PII
- DoDD 5400.11 establishes the DoD policy that:
 - 4.1. The privacy of an individual is a personal and fundamental right that shall be respected and protected
 - 4.1.1. The DoD's need to collect, maintain, use, or disseminate personal information about individuals for purposes of discharging its statutory responsibilities shall be balanced against the right of the individual to be protected against unwarranted invasions of their privacy



DoD Privacy Regulations

- It is also DoD policy that:
 - 4.1.2. The legal rights of individuals, as guaranteed by Federal laws, regulations, and policies, shall be protected when collecting, maintaining, using, or disseminating personal information about individuals
 - 4.1.3. DoD personnel, to include contractors, have an affirmative responsibility to protect an individual's privacy when collecting, maintaining, using, or disseminating personal information about an individual



General Privacy Protection

C1.4.1. General Responsibilities. DoD Components shall establish appropriate administrative, technical, and physical safeguards to ensure that the records in each system of records are protected from unauthorized access, alteration, or disclosure and that their confidentiality is preserved and protected. Records shall be protected against reasonably anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is kept.



Federal Privacy Overview

Civil Liberties Protection

DoD 5400.11-R also requires:

- C1.1.5. Exercise of First Amendment Rights
 - C1.1.5.1. Do not maintain any records describing how an individual exercises his or her rights guaranteed by the First Amendment of the U.S. Constitution, except when:
 - C1.1.5.1.1. Expressly authorized by Federal statute;
 - C1.1.5.1.2. Expressly authorized by the individual; or
 - C1.1.5.1.3. Maintenance of the information is pertinent to and within the scope of an authorized law enforcement activity
 - C1.1.5.2. First Amendment rights include, but are not limited to, freedom of religion, freedom of political beliefs, freedom of speech, freedom of the press, the right to assemble, and the right to petition



Federal Privacy Overview

Summary

- You should now be able to:
 - Discuss how the Privacy Act is implemented within the MHS and its impact on those who solicit and collect records of PII on behalf of the TMA
 - Describe how DoD employees and contractors can be held accountable for misuse or mishandling of PII
 - Define other federal regulations that outline privacy requirements when collecting PII



Federal Privacy Overview

Resources

- <http://tricare.mil/tma/privacy/RegulatoryRequirementsGuidanceResources.aspx>
- Federal Law
 - 5 U.S.C 552a, the Privacy Act of 1974, as amended
- DoD
 - DoDD 5400.11, DoD Privacy Program, May 8, 2007, Incorporating Change 1, September 1, 2011
 - DoD 5400.11-R, Department of Defense Privacy Program, May 14, 2007
- TMA Privacy Office Web site:
<http://www.tricare.mil/privacy/>



Federal Privacy Overview

Resources

- <http://www.tricare.mil/tma/privacy/mailinglist.aspx> to subscribe to the TMA Privacy and Civil Liberties Office E-News
- TMA Tools for Related Questions:
<http://www.tricare.mil/tma/privacy/Hipaa.aspx>
- DoD Privacy and Civil Liberties Office:
<http://dpclo.defense.gov/privacy>
- TMA Incident Response Team and Breach Notification Administrative Instruction, November 5, 2009
<http://www.tricare.mil/tma/privacy/downloads/TMA-BreachResponseAdministrativeInstruction.pdf>
- TMA Breach Reporting:
<http://www.tricare.mil/TMA/Privacy/breach.aspx>



Federal Privacy Overview

Resources

- OMB
 - OMB Circular No. A-130 Revised
 - OMB Memorandum 99-05, Attachment B (Privacy and Personal Information in Federal Records)
- Office of the Secretary of Defense (OSD)
 - OSD Administrative Instruction No. 81, OSD/Joint Staff (JS) Privacy Program, November 20, 2009



TMA Privacy Contacts

- Please contact the Director of the TMA Privacy and Civil Liberties Office for any questions



Conclusion

- Treat the privacy information of others as you would wish your privacy information to be safeguarded and kept confidential
- Be as careful with it as you would your own \$1000 bill
- It is the law, and it is the right thing to do

