Office of the Chief Information Officer
Office of the Assistant Secretary for Administration
Department of Health and Human Services

United States Department of Health and Human Services Information Sharing Environment (ISE) Privacy Policy

May 29, 2013

Project:	HHS OCIO Policy
Document Number:	HHS-OCIO-2013-0002

Contents

I. Purpose

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) directed the President to establish "an approach that facilitates the sharing of terrorism information," which includes information about weapons of mass destruction, homeland security information, and law enforcement information (referred to collectively as "terrorism-related information"), among and between federal, state, local, and tribal agencies and entities, the private sector, and our foreign partners in order to detect, prevent, disrupt, preempt, and mitigate the effects of terrorism on the United States.[1] This approach to information sharing is called the Information Sharing Environment (ISE). IRTPA also directed the President to develop and adopt policies and procedures governing the use of information in the ISE, including guidelines to "protect privacy and civil liberties in the development and use of the ISE."[2]

The Information Sharing Environment (ISE) is designed to facilitate the sharing of weapons of mass destruction information, homeland security information, and law enforcement information (herein referred to collectively, "terrorism-related information." See definitions in Appendix A) among federal agencies participating in the ISE. Sharing is enabled via a combination of information sharing policies, procedures, and technologies. The ISE enables enhanced information sharing, information access, and collaboration to combat terrorism, and will do so while protecting information privacy and civil liberties.

The Program Manager for the ISE issued *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment* that were approved by the President on December 4, 2006, and requires federal entities participating in the ISE to have a written privacy protection policy that implements the Guidelines. This document constitutes the Department of Health and Human Services' (HHS) compliance with that requirement.

This document comprises HHS policies and procedures that ensure the collection, use, sharing, storage, and security of information that is both terrorism-related information and "protected information (PI)" (See definitions in Appendix A) shared through the ISE and is consistent with the ISE Privacy Guidelines. Where possible, this document identifies existing HHS policies and procedures that meet the privacy requirements of the ISE. Where necessary, however, this document also creates policies specific to the activities and resources that HHS will devote to the ISE.

HHS will implement this policy to facilitate sharing and disclosure of PI and personally identifiable information (PII) in the ISE.

[1] Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. 108-458, 18 Stat. 3665, § 1016(a)(2) (Dec. 17, 2004).

[2] IRTPA at § 1016(b)(1). See An Introduction to the ISE Privacy Guidelines (Dec. 4, 2006), available at http://www.ise.gov/docs/privacy/PrivacyGuidelines20061204.pdf. See also ISE Goals, available at http://www.ise.gov/pages/vision.html.

II. Scope

This policy applies to all activities undertaken by the Department of Health and Human Services ("HHS" or "Department") related to the collection, use, storage, or disclosure of terrorism-related PI in the ISE. It also applies to HHS employees, vendors and contractors that access, use or disclose any PI and/or PII with participants in the ISE. HHS follows the Privacy Act's requirement with regard to systems of records containing protected information (PI). HHS also recognizes that some of its systems will contain information on US citizens, lawful resident aliens, and others who are not covered by the Privacy Act. In cases where these individuals request redress, HHS will voluntarily disclose this information if it can, and extend an opportunity for redress to all subjects of records whose PII is collected, stored, or disclosed from its information systems, including undocumented immigrants and foreign nationals who are not lawful permanent residents. HHS reconfirms, however, that persons other than "individuals," as that term is defined under the Privacy Act, do not have these rights under the Privacy Act, and that HHS is under no legal obligation to make these disclosures.

This policy is limited in scope, and only covers certain types of information. ISE is concerned with information systems where terrorism-related information and other information are commingled ("Category II systems"), and are also systems that contain information about both U.S. persons and non-U.S. persons ("mixed systems"). HHS has very few systems that are both "Category II" and "mixed" systems. In many systems, HHS maintains information on both "individuals" as described by the Privacy Act and information on other persons as well, and so those systems meet the definition of "mixed systems," but the PI is not terrorism-related, and therefore those systems are not also "Category II systems." This policy covers only those very few HHS systems that are both mixed systems and Category II systems, which means these systems contain at least some records that:

1. Are about natural persons, and
2. Are about both individuals under the Privacy Act;
3. Are about other persons who are not individuals under the Privacy Act, and
4. Contain some terrorism-related information.

These systems include our "Suspicious Activity Report" (SAR) systems, and may include other types of data or other systems.

This document acknowledges both statutory and regulatory standards with which HHS is required to comply and best practices that HHS has determined are essential to providing adequate protection to the PII that the Department collects and shares in the ISE.

Under Section 4 of HHS's *HHS-OCIO Policy for Information Systems Security and Privacy (IS2P),* HHS Operating Divisions (OpDivs) and Staff Divisions (StaffDivs) may "decide whether to issue any additional OpDiv/StaffDiv-wide security controls for OpDiv/StaffDiv information systems to augment the government and Department-wide

controls" specified in the IS2P. Information assurance and privacy activities conducted within the Department shall be consistent with the guidance, methodologies, and intent prescribed by the National Institute of Standards and Technology (NIST) Special Publication (SP) series and other relevant federal laws and guidance documents.[3] However, the IS2P also permits OpDivs and StaffDivs to implement "compensating controls" (security measures that provide protection to HHS information and assets equal to those prescribed by the IS2P), provided that certain other conditions are met.[4]

III. Goal

HHS' privacy policies, including this ISE Privacy Policy, facilitate the collection and use of PII (including PI):

1. To achieve the lawful purpose(s) for which the data were collected, and
2. To meet HHS's responsibilities in protecting the health of all Americans and providing essential human services, especially for those who are least able to help themselves,
3. While protecting the privacy, civil rights, and civil liberties of U.S. citizens and lawful permanent residents.

In addition to the requirements set forth in this policy, HHS will continue to comply with the Constitution and all applicable laws and Executive Orders relating to PI, privacy, and information sharing. [5] HHS will identify and assess laws, Executive Orders, policies, and procedures applicable to the PI that HHS will make available in the ISE, and will, on a continual basis, implement updated policies and procedures to address any new or changing requirements.

IV. Definitions and Authorities

See Section VII – Definitions and Section VIII – Authorities.

V. Policy

HHS maintains high standards for the protection of PII, including PI shared in the ISE. HHS charges its Senior Agency Official for Privacy (SAOP) with ensuring the proper implementation of information privacy protections, including full compliance with federal laws, regulations and policies relating to information privacy, such as the Privacy Act of 1974 (Privacy Act), and the e-Government Act of 2002.

[3] HHS Office of the Chief Information Officer, *HHS-OCIO Policy for Information Systems Security and Privacy (IS2P)*, §4.1.4 (July 7, 2011).
[4] IS2P §4.2.2.
[5] Many of these current authorities are included in Section VII of this document, Authorities. Among the most significant of these are the e-Government Act of 2002 (including the Federal Information Security Management Act (FISMA)); the Privacy Act of 1974; the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and its implementing Privacy and Security Rules; and Memoranda issued from the Office of Management and Budget including 03-22, 05-08, 07-16, 10-22, and 10-23.

A. Collection (Acquisition and Access)

HHS collects PII consistent with the procedures set out in its IS2P Handbook, Section 1.11 (Privacy). These procedures include protections ensuring that individuals may expressly or implicitly consent to the terms and conditions in privacy notices[6] and that individuals may learn how their information is to be used.[7] HHS observes the principle of collecting only the minimum necessary information in order to carry out the purpose of the data collection.[8] The IS2P Handbook also requires HHS to ensure that individuals are informed of the authority for collecting the information (i.e., the statute or Executive Order), as well as whether information collection is mandatory or voluntary, and of the purpose for collecting that information.[9] OpDivs and StaffDivs assess information collection practices at every stage of an information collection process. The IS2P Handbook states that prior to beginning a new or modified collection effort, OpDivs and StaffDivs must:

1. Complete a privacy impact assessment (PIA) or privacy threshold assessment (PTA), including:
    a. Determining if the system requires and has an appropriate system of records notice (SORN), consistent with the Privacy Act
    b. Determining if the system requires and has an appropriate information collection approval number from the Office of Management and Budget (OMB), consistent with the Paperwork Reduction Act (PRA)
2. Conduct a privacy requirements analysis, including:
    a. Identifying data needs and sources
    b. Incorporating privacy requirements into requests for proposals (RFP), statements of work (SOW), and contracts
3. Conduct a privacy risk analysis, including:
    a. Identifying system privacy risks
    b. Documenting system privacy weaknesses
4. Consider costs related to implementing privacy controls, and generate any required cost reports to document these costs
5. Select and develop privacy controls, including implementing appropriate privacy controls for new and existing systems
6. Develop a privacy plan, which must include:
    a. Developing training and awareness for all employees and persons working on behalf of HHS involved in managing, using and/or operating information systems, including role-based training for those that handle PII
    b. Developing relevant documents and guides, and

[6] HHS Office of the Chief Information Officer, *HHS-OCIO Policy for Information Systems Security and Privacy Handbook (IS2P Handbook)*, §1.11 (Privacy, P-PRIV.1).
[7] IS2P Handbook §1.11 (Privacy, P-PRIV.2).
[8] IS2P Handbook, §1.11 (Privacy, P-PRIV.3).
[9] IS2P Handbook, §1.11 (Privacy, P-PRIV.2).

7. Review the privacy plan (as described in (6), above).[10]

HHS also maintains regulations in the Code of Federal Regulations governing its collection and use of PII.[11] For example, no record is maintained in the Department unless:

1. it is relevant and necessary to accomplish a Department function required to be accomplished by statute or Executive Order[12]
2. HHS has received approval from OMB for the collection of information in the record, in compliance with the Paperwork Reduction Act, if applicable;[13]
3. it is acquired to the greatest extent practicable from the subject individual when maintenance of the record may result in a determination about the subject individual's rights, benefits or privileges under Federal programs;[14]
4. A Privacy Impact Assessment (PIA) has been conducted, if it is required for the information collection. Under Section 1.15 of the IS2P Handbook, HHS conducts PIAs on each Department system as a method to evaluate inherent privacy risks.
5. The OpDiv or StaffDiv Senior Official for Privacy has reviewed and approved a Privacy Impact Assessment (PIA) for the relevant system.[15]

B. Notice

HHS maintains regulations stating that for every system of records, where the information in the record is collected from the subject of the record, the individual must be informed of the authority for providing the information, whether providing the information is mandatory or voluntary, the principal purpose for maintaining the information, the "routine uses" for which the record may be disclosed outside the agency, and the consequences of refusal to provide the information, if any. Further, HHS regulations state that individuals may request to know whether a system of records contains information about them, and may at the same time request access to any records pertaining to them.[16]

[10] HHS Cybersecurity Program, *Privacy in the System Development Life Cycle (SDLC)* (January 16, 2007).
[11] See e.g., HHS Privacy Act regulations at 45 CFR 5b.
[12] 45 CFR 5b.4(a)(1)
[13] *See* Paperwork Reduction Act, 44 USC § 3501 *et seq.*; OMB's implementing regulations, "Controlling Paperwork Burdens on the Public, 5 C.F.R. Part 1320. A variety of helpful guidance regarding Paperwork Reduction Act compliance can be found at OMB's web site, <http://www.whitehouse.gov/omb/inforeg_infocoll/>
[14] 5 USC 552a(e).
[15] IS2P, §§5.16.10 and 5.16.11.
[16] 5 USC 5b.4 and 5.

C. Acceptable Use

Individuals must be notified of the law authorizing the creation of a system of records for each collection of PII by HHS.[17] Prior to using any PII in a system of records, system owners, with the assistance of their Senior Officials for Privacy (SOPs), shall verify that:

1. A system of records notice (SORN) has been developed and is maintained as required by the Privacy Act of 1974.
2. The SORN has been published on the public-facing HHS web site. [18]
3. If the use is part of a computer matching program, confirm that the program meets all computer matching requirements listed in the Privacy Act, as amended.[19]
4. Individuals have consented to the collection and use of their PII, unless the agency is required to collect the PII by statute or Executive Order to be provided by the individual.[20]
5. PI shared by HHS in the ISE will be used only in a manner that is consistent with the authorized purposes of the ISE.[21]

D. Data Quality and Integrity

HHS maintains a set of guidelines entitled *HHS Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated to the Public* (HHS Information Quality and Integrity Policy). These guidelines have the ultimate goal of ensuring that information HHS provides to the public is accurate, timely and useful. The guidelines integrate the principle of information quality into every phase of information development, including creation, collection, and maintenance, as well as dissemination.

Each OpDiv and Staff Div at HHS maintains its own mission-specific data quality and integrity policy, consistent with OMB's *Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies* (October 1, 2001, amended February 22, 2002). Each of these OpDiv and StaffDiv policies contains the following elements:

1. The mission of the agency
2. The scope and applicability of the guidelines within the agency
3. The types of information that the agency disseminates
4. The dissemination methods employed by the agency
5. The policies, standards and practices that the agency employs to ensure the quality of the information it disseminates

[17] IS2P Handbook, §1.11 PRIV.2.
[18] IS2P Handbook, §1.11 P-PRIV.7.
[19] HHS, *Department of Health and Human Services Data Integrity Board* Charter (revised February 8, 2002) and *HHS Data Integrity Board Guidelines for Computer Matching Agreements* (revised February 1, 2002).
[20] 45 CFR 5b.4(a)(3)
[21] 45 CFR 5b.4(a)(1)

6. An administrative mechanism and contact points for each agency so that individuals may seek correction of any information that is believed not to meet the OMB, HHS, or agency-specific guidelines, and
7. An administrative appeals process.

Each OpDiv and StaffDiv that supplies information in the ISE will follow these guidelines before transmitting, disclosing, or disseminating information in the ISE. If officials receive later knowledge, and determine the information is not accurate, complete, timely and relevant they will:

1. Correct (or update) the information in each record or file where it appears
2. Use the accounting of disclosures, if any, to identify previous recipients of information, and provide updated or corrected information if appropriate and possible, and
3. Refrain from using or disclosing inaccurate or out of date information.

Whenever possible, each OpDiv and StaffDiv that provides information in the ISE will identify whether each data subject in any records shared in the ISE is an "individual" as that term is defined by the Privacy Act. HHS will update each data recipient in the ISE if HHS later learns of a change in the person's status (i.e., whether that person is a US citizen, lawful permanent resident, or person with some other status).[22]

E. Sharing and Dissemination[23]

HHS regulations state that the Department will maintain no Privacy Act record unless it is relevant and necessary to accomplish a Department function required to be accomplished by statute or Executive Order. Therefore, no records will be made available in the ISE unless they have been lawfully obtained,[24] and are authorized to be lawfully shared and disseminated in the ISE pursuant to a published "routine use."[25]

Before disclosing PI and/or PII to another agency that is a participant in the ISE, each OpDivs/StaffDivs must review all PI and PII, in order to:

[22] See, e.g., 5 USC 552a(c)(4): "Each agency, with respect to each system of records under its control, shall… inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.

[23] Currently, the predominant way HHS shares information in the ISE is by using the Guardian information system to transmit information to the Federal Bureau of Investigation (FBI). HHS does not use Guardian to disclose information to any other ISE participant. The FBI reviews that information to verify whether it may be "terrorism related," gauges whether the reliability of the data is limited, and determines whether further legal protections may apply to the PI or PII and whether it must be labeled as such before further disclosed. The FBI then shares the PI or PII with other participants in the ISE, if warranted. HHS will, however, attempt to maintain the integrity of the process to the best of its ability, as well, by providing metadata where relevant and available.

[24] 5 USC 552a(e)(1) and 45 CFR 5b.4.

[25] 5 USC 552a(b)(3).

1. Verify, to the best of its ability, that any PI and PII to be disclosed from Category II systems is relevant to terrorism-related information as defined by the ISE.
2. Ensure that any HHS employee personnel information will be disclosed only in accordance with appropriate privacy protections as required by law (e.g., the Privacy Act of 1974). The Deputy Assistant Secretary of the Office of Human Resources is responsible for defining policies and procedures for protecting employee data and communicating those policies to all personnel who come in contact with personnel information.
3. Make reasonable efforts to assure that all records are accurate, complete, timely, and relevant for agency purposes. [26]
4. Identify the nature of the PI being shared, to the extent of the functionalities and format of the information dissemination tool or process.
5. Label all shared PI, to the extent the functionalities and format of the dissemination tool or process allows, to indicate the level of confidence associated with the PI.

Before sharing PI, HHS staff must determine whether information submitted constitutes "terrorism-related information." Any HHS staff member that needs to make this determination must consider whether the information reflects one of sixteen "Defined Criminal Activity and Potential Terrorism Nexus Activities" or "Potential Criminal or Non-Criminal Activities Requiring Additional Fact Information during Investigation." HHS staff will complete this analysis before any suspicious activity report (SAR), Information Sharing Environment Suspicious Activity Report (ISE-SAR), or other information is disseminated.[27] HHS will, however, also rely on the expertise and insight of the FBI, which will also conduct this review before further sharing data with the ISE participants.

HHS is aware that special concerns arise when analysts have the ability to combine information from two different sources about the same subject of a record. In these situations, inadvertently combining information about two different subjects of records (for example, in cases where two subjects of records have the same name) can have significant negative consequences for those subjects of records, especially in cases where they may incur liability or culpability. Therefore, HHS staff sharing PI will make an effort to:

1. Avoid merging or combining records if there is any possibility the two or more records are those of different subjects of records (e.g., where records contain only partial matches)
2. Merge records only where each record contains an individual identifier (e.g., a social security number (where authorized and appropriate), a policy number, or other identifier that only one subject of a record is likely to hold)
3. Where HHS appears to hold multiple records on the same person requested by participants in the ISE, but there is a risk of error, provide these records

[26] 5 USC 552a(e)(5).
[27] Information Sharing Environment (ISE) Functional Standard (FS), Suspicious Activity Reporting (SAR), version 1.5. ISE-FS 200 (2009), Part B, "ISE-SAR Criteria Guidance."

separately, with an indication of the possibility they refer to the same person noted where possible.

When providing PII or any information covered by this policy to other agencies, HHS will provide updates to that information if it is found to be incomplete or inaccurate, especially when deficiencies in the information may affect the rights, benefits, privileges, or obligations of any subject of a record. Conversely, in the event that HHS receives information including PI from participants in the ISE and determines it to be inaccurate (incorrectly merged, incomplete, erroneous, or in any other way deficient), HHS will contact the providing agency and advise its ISE Privacy Official of the need to update or correct such records.

F. Access and Amendment

In order to ensure the accuracy of systems of records maintained by HHS, HHS regulations permit subjects of records to access their records and contest information about themselves.[28] Under these regulations, subjects of records may request that records about themselves be amended if they believe the records are not accurate, timely, relevant, or complete enough to assure fairness to the subject of the record. Subjects of records making amendment requests shall address them to the responsible Department official in writing, or may make requests in person, and the responsible Department official may amend the records at that time.

G. Redress

If the subject of a record has complaints or objects to the accuracy, relevance, timeliness, or completeness of PI about himself or herself allegedly acquired, accessed, stored, or shared by HHS, the subject of a record may request that HHS amend the record.[29]

In some cases, the subject of a record may suffer some legal harm or restriction, and may suspect that this is due to the existence of incorrect or incomplete information in his or her record; but HHS will not be able to disclose the information in the record due to a mandatory exemption from disclosure. In these conditions, the subject of a record may be able to request the record be corrected or amended, even if he or she is not able to view the record and confirm his or her assumptions. In these cases, HHS will in fact make the amendment or correction if doing so is reasonable and appropriate.

HHS will offer the opportunity of redress to subjects of records, including those that do not have the right to redress under the Privacy Act. HHS recognizes that some of its systems will contain information on persons who are not considered to be "individuals" under the Privacy Act. HHS will use its ability to exercise discretion to disclose information and extend an opportunity for redress to all subjects of records whose PII is collected, stored, or disclosed from its information systems, including undocumented

[28] 45 CFR 5b.
[29] 45 CFR 5b.7(a).

immigrants and foreign nationals who are not lawful permanent residents and therefore not "individuals" under the Privacy Act.

1. The request must be in writing and may be addressed to the System Manager as indicated in the relevant SORN, to the Department's FOIA Office, or to the Privacy Act Officer. This point of contact must process the request in coordination with the OSSI's ISE Officer. In the alternative, if feasible, the subject of the record may make the request in person and the responsible Department official may correct or amend the record at that time.
2. A request for correction or amendment of a record will be acknowledged within 10 working days of receipt unless the request can be processed and the subject of the record informed of the responsible Department official's decision, where appropriate, within that 10 day period.[30]
3. The Department official will review the PI in question and will, within a reasonable time:
   a. confirm that the information is complete and accurate; or
   b. determine that the information is incomplete and inaccurate and correct it; or
   c. purge the information if the Department official determines the PI is no longer relevant or necessary to accomplish a Department function.[31]
4. All previous recipients of the record, a list or which will be maintained in the system's accounting of disclosures, will be informed of the corrective action taken,[32] including any recipients that are participants in the ISE, per the policy for ensuring data quality and integrity noted in Section 5.D., above.

H. Security

HHS is required to provide adequate and effective security protection for all PII, including PI shared in the ISE, and in records stored and accessed in HHS systems, to ensure their protection from unauthorized access, use, modification, or destruction. Each OpDiv and StaffDiv develops policies and procedures to implement the protections for their systems that store PI. Among other provisions of the IS2P Policy and Handbook are requirements that ensure that:

1. Information systems maintain adequate, risk-based protections in the control areas defined in Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information Systems* (March, 2006).[33]
2. Information assurance and privacy activities conducted within the Department are consistent with the guidance, methodologies, and intent prescribed by the NIST SP series and other relevant federal laws and guidance documents, such as the Federal Information Security Management Act of 2002 (FISMA); OMB Circular

[30] 45 CFR 5b.7(b).
[31] 45 CFR 5b.7(c).
[32] 45 CFR 5b.7(d).
[33] IS2P, §3.1.3

A-130, Appendix III; applicable NIST security guidance; and Departmental security policies and procedures.[34]

3. Records are maintained according to a designated file structure, as specified in approved records schedules.
4. Security protection is commensurate with the risk and magnitude of harm HHS or the record subject would face in the event of a data security breach.[35]
5. OpDivs and StaffDivs obtain written authorization from management in the form of Interconnection Security Agreements or Data Sharing Agreements that do not conflict with or otherwise contradict Department IT security and privacy policies, procedures, controls, standards, applicable legislation, regulation, guidance, or contractual obligations.[36] HHS presumes other agencies comply with the Federal Information Security Management Act; HHS does not have the resources to monitor other agencies' data handling procedures.

I. Accountability, Enforcement, and Audit

In order to ensure the accountability and protection of PI and all PII shared in the ISE, HHS employs the following enforcement and audit procedures:

1. HHS requires that OpDivs document, maintain, and communicate policies and procedures,[37] in accordance with the *HHS Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response* and HHS-OCIO020080-0001.003, *HHS Policy for Responding to Breaches of Personally Identifiable Information*.
2. HHS requires its Privacy Incident Response Team (PIRT) to "evaluate response activities to ensure that implementation is commensurate with the impact to the individual, the OpDiv or StaffDiv, and the Department, and complies with applicable law(s)."[38]
3. HHS requires its Information Security and Privacy Program to "ensure that suspected or confirmed breaches of PII on systems owned or operated by the Department, including those owned or operated by federal contractors or grantees on behalf of the Department, are identified, tracked, and responded to in an effective, consistent, and timely manner."[39]HHS requires OpDivs and StaffDivs to develop, disseminate, and periodically review and update formal, documented audit and accountability policy statements and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination, and compliance.[40] HHS will advise its OpDivs to review these policies and incorporate, where necessary, references to the ISE guidelines and this ISE Privacy Policy.

[34] IS2P, §4.1.4
[35] IS2P, §4.1.3.
[36] IS2P Handbook, §1.16 (Interconnection Sharing Agreement/Data Sharing, P-ISA.1).
[37] *HHS Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response* and HHS-OCIO020080-0001.003, *HHS Policy for Responding to Breaches of Personally Identifiable Information*.
[38] *HHS Policy for Responding to Breaches of Personally Identifiable Information, Sec. 4.3.*
[39] *HHS Policy for Responding to Breaches of Personally Identifiable Information, Sec 4.3.*
[40] IS2P Handbook, §1.21 (Audit and Accountability) P-AU.1 and P-AU.2.

4. HHS has designated the Office of Security and Strategic Information (OSSI) as the Federal Intelligence Coordinating Office (FICO) and the Director of OSSI as the ISE official to receive reports (or copies, as appropriate) regarding ISE, to include alleged errors, later discovered in PI that was shared in the ISE from HHS.
5. HHS requires OpDivs and StaffDivs to develop performance measures and metrics to evaluate the effectiveness of IT security and privacy policies, procedures, and controls.[41]
6. The HHS Office of the Inspector General (OIG) reviews HHS programs and activities, including HHS' participation in the ISE, to promote effectiveness and prevent abuse.

J. Training

HHS maintains a policy requiring OpDivs and StaffDivs to develop a formal, documented, training policy regarding security and privacy awareness.[42] OpDivs and StaffDivs must disseminate, periodically review, and, as necessary, update the training policy. The Chief Information Officer's (CIO's) office will provide security awareness for all employees and other persons working on behalf of HHS that are involved in managing, using, or operating information systems, including contractors.[43] The CIO's office will provide privacy awareness training prior to granting access to Department systems and networks, and annually thereafter.

HHS will provide supplemental training for employees, vendors and contractors that will use systems to collect, maintain, or disclose information that may ultimately be shared in the ISE. HHS will train these staff members on the requirements of this ISE Privacy Policy, including the procedures for reporting violations of this policy. At the conclusion of the training, participants will either be provided with a copy of the policy or be informed how to access it electronically.

Training includes explanations of the importance and responsibility in safeguarding PII and ensuring privacy, as established in federal legislation and OMB guidance. The HHS SAOP is responsible for ensuring that all of the Department's employees and contractors receive appropriate privacy training.[44] Furthermore, OpDiv Chief Information Security Officers (CISOs) are assigned to support general privacy awareness and role-based training activities for all personnel using, operating, supervising, or managing information systems. Senior Officials for Privacy (SOPs) must coordinate privacy education and awareness activities and ensure that activities appropriate to their division are established for personnel using, operating, supervising, or managing information systems.

1. The following authorities require HHS personnel training:

[41] IS2P Handbook, §1.4 (Performance Measurement, P-PM.1).
[42] IS2P Handbook, §1.28 (Awareness and Training) P-AT.1.
[43] IS2P Handbook, §1.28 (Awareness and Training) P-AT.2.
[44] IS2P, §5.9.13.

a. Subsection (e)(9) of the Privacy Act of 1974, which requires employee training on the requirements of the Privacy Act.
b. OMB Memorandum M-01-05, *Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy,* reiterates training required by the Privacy Act and emphasizes the need to communicate accountability and penalties under the law.
c. OMB Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy,* requires training for employees and contractors regarding information privacy laws, regulations, policies, and procedures governing the agency's handling of PII.
d. Section 9.b. of the ISE Privacy Guidelines requires each agency to "develop an ongoing training program in the implementation of these Guidelines, and . . . provide such training to agency personnel participating in the development and use of the ISE."

2. The CIO's office has developed Departmental guidance for use by each OpDiv and StaffDiv in implementing annual training. OpDivs and StaffDivs may develop their own training programs, provided they are consistent with legal requirements.
3. Privacy awareness training shall be required of Department employees and contractors before granting initial access to HHS systems and networks, and annually thereafter.[45] The training will explain the importance of, and responsibility for safeguarding PII and ensuring privacy, as established in federal legislation and OMB guidance.[46]
4. Current privacy awareness training includes modules on defining privacy; the consequences of violating privacy; protecting PII; breach reporting; transparency; individual participation/redress; purpose specification; data minimization and retention; use limitation; data quality and integrity; and security.

K. Awareness

HHS will take steps to publicize appropriate notice of its policies and procedures for implementing these Guidelines and will make this policy publicly available on its web site and individually on request.

L. Required Procedures

HHS has developed Departmental procedures, located on the HHS intranet, to comply with many privacy- and security-related regulatory requirements. OpDivs and StaffDivs may customize the Departmental procedures or develop their own, as needed, to meet their local needs, provided they are consistent with Departmental procedures and all applicable legal requirements.

[45] IS2P Handbook, §1.28 (Awareness and Training) P-AT.4.
[46] IS2P Handbook, §1.28 (Awareness and Training, P-AT.4).

The Privacy Act of 1974 requires the Department to promulgate regulations[47]:

1. Establishing procedures whereby a subject of a record can be notified in response to his request if any system of records named by the subject of the record contains a record pertaining to him;[48]
2. Defining reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual;[49]
3. Establishing procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him;[50]
4. Establishing procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to be able to exercise fully his rights under this section;[51] and
5. Establishing fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record.[52]

M. Assessment of Policies and Update of Privacy Policy

The Deputy Assistant Secretary for Information Technology and Chief Information Officer, under the authority delegated by the Assistant Secretary for Administration, ensures that the Department is in compliance and conformance with Public Laws, regulations, policies, guidance (e.g., from OMB or GAO), standards, procedures, and instructions concerning privacy, security, and data management as these pertain to the ISE.[53] This activity may require updating Department policies, including this policy, as necessary to respond to evolving laws, policies and procedures.

VI. Responsibilities

A. The Senior Agency Official for Privacy (SAOP)

The Senior Agency Official for Privacy (SAOP) is responsible for:

[47] 5 USC 552a(f).
[48] 5 USC 552a(f)(1).
[49] 5 USC 552a(f)(2).
[50] 5 USC 552a(f)(3).
[51] 5 USC 552a(f)(4).
[52] 5 USC 552a(f)(5).
[53] HHS Office of the Chief Information Officer, *HHS Policy for Information Technology (IT) Policy Development*, §5.1 (November 28, 2006).

1. Ensuring the proper implementation of information privacy protections, including full compliance with Federal laws, regulations, and policies relating to information privacy.
2. Maintaining appropriate documentation regarding compliance with information privacy laws, regulations, and HHS policies.
3. Overseeing, coordinating, and facilitating the Department's privacy compliance efforts, including reviewing documented information privacy procedures to ensure comprehensiveness and currency, and coordinating any necessary revisions.
4. Ensuring that data sharing activities occur within applicable privacy laws and with appropriate safeguards.
5. Providing education programs regarding the information privacy laws, regulations, policies, and procedures governing the Department's handling of PII.

As part of fulfilling these enumerated duties, the SAOP must ensure that protections are implemented through efforts such as training, business process changes, and system designs. The SAOP must identify and implement technologies to enhance privacy, such as construction of access control lists (ACLs) to manage system access authorizations, hashing, data anonymization, immutable audit logs, and authentication, where appropriate.

B. System Owners

System owners are responsible for:

1. Conducting a Privacy Impact Assessment (PIA) on each system for which they are responsible, in coordination with their respective SOP, especially if the system maintains information on individuals or when the Department develops, acquires, or buys new systems to handle PII.
2. Conducting assessments of the risk and magnitude of harm that would result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information in any system that supports the Department's critical operations, at no less than every three years or when significant changes occur to the system or the network to which it is connected.
3. Ensuring proper physical, administrative, and technical controls are in place to protect PII found in the system.

C. Senior Officials for Privacy (SOPs)

OpDiv and Staff Div Senior Officials for Privacy (SOPs) are responsible for:

1. Supporting the Department SAOP in privacy reporting activities, as necessary, including the maintenance of, and compliance with, presidential mandates and FISMA reporting activities.

2. Establishing and implementing division privacy policies, procedures, and practices consistent with Department privacy requirements, in coordination with the OpDiv CIO and Chief Information Security Officer (CISO).
3. Coordinating OpDiv policy, guidance, and system-level documentation to ensure that Department management, technical, and operational privacy requirements are addressed.
4. Establishing an OpDiv policy framework to facilitate the development and maintenance of PIAs for all systems based on department and Federal legislative requirements.
5. Reviewing completed OpDiv PIAs and attesting to their adequacy and accuracy.
6. Coordinating activities to review regularly PII holdings, assess the risk associated with PII holdings, recommend controls to protect the confidentiality of the PII, and eliminate the unnecessary use or collection of PII (including Social Security numbers).
7. Coordinating with the OpDiv Privacy Act Contact to ensure that all required SORNs are completed and published in the *Federal Register*, and also on the HHS.gov web site.

D. Federal Employees and Contractors

All HHS employees and contractors are responsible for:

1. Complying with the Department's policies, standards, and procedures.
2. Familiarizing themselves with any special requirements of their positions for accessing, protecting, and using data, including Privacy Act records, copyrighted materials, trade secrets, or procurement-sensitive information.
3. Reporting any suspected or actual computer security incidents, including the loss of control of PII and PHI, immediately to the OpDiv Computer Security Incident Response Team, or, if none, to the Department Privacy Incident Response Team.
4. Reading, acknowledging, signing, and complying with the HHS Rules of Behavior, as well as any OpDiv, StaffDiv or system-specific Rules of Behavior, before gaining access to the Department's systems and networks.
5. Completing required privacy and security awareness training.

VII. Effective Date/Implementation

The effective date of this policy is the date the policy is approved.

Requirements stated in this policy are consistent with law, regulations, and other Department policies applicable at the time of its issuance. Actions taken to implement this policy must comply with the requirements of pertinent laws, rules and regulations, as well as the lawful provisions of applicable negotiated agreements for employees in exclusive bargaining units.

The HHS policies contained in this issuance shall be exercised in accordance with Public Law 93-638, the Indian Self-Determination and Education Assistance Act, as amended, and the HHS Secretary's policy statement dated August 7, 1997, as amended, titled "Department Policy on Consultation with American Indian/Alaska Native Tribes and Indian Organizations." It is HHS policy to consult with Indian people to the greatest practicable extent and to the extent permitted by law before taking actions that affect these governments and people; to assess the impact of the Department's plans, projects, programs, and activities on tribal and other available resources; and to remove any procedural impediments to working directly with tribal governments or Indian people.

VIII. Approved

___/s/Frank Baitman/s/_____ May 29, 2013
Frank Baitman DATE
HHS Chief Information Officer (CIO)
HHS Senior Agency Official for Privacy (SAOP)

IX. Definitions

Homeland Security Information, as derived from the Homeland Security Act of 2002, Public Law 107-296, Section 892(f)(1) (codified at 6 USC § 482(f)(1)), is defined as any information possessed by a state, local, tribal, or federal agency that:

- Relates to a threat of terrorist activity;
- Relates to the ability to prevent, interdict, or disrupt terrorist activity;
- Would improve the identification or investigation of a suspected terrorist or terrorist organization; or
- Would improve the response to a terrorist act.

Individual has the same meaning as at 5 USC § 552a(a)(2), "a citizen of the United States or an alien lawfully admitted for permanent residence."

Information Sharing Environment (ISE) has the same meaning as defined in the Intelligence Reform and Terrorism Prevention Act of 2004, as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007 (IRTPA), 6 USC§ 485 et seq., which describes the ISE as an approach to the sharing of information related to terrorism that is being implemented through a combination of policies, procedures, and technologies designed to facilitate the sharing of critical information by all relevant entities. The ISE serves the dual imperatives of enhanced information sharing to combat terrorism and protecting the information privacy and other legal rights of Americans in the course of increased information access and collaboration. The ISE is being developed by bringing together, aligning, and building upon existing information sharing policies and business processes and technologies (systems), and by promoting a culture of information sharing through greater collaboration. It is being developed pursuant to Section 1016 of (IRTPA) and Executive Order 13388, entitled "Further Strengthening the Sharing of Terrorism Information to Protect Americans."

Law Enforcement Information has the same meaning as defined in the ISE's *Guideline 2 Report: Departments and Agencies and State, Local, and Tribal Governments, Law Enforcement Agencies, and the Private Sector* as any information obtained by or of interest to a law enforcement agency or official that is both:

- Related to terrorism or the security of our homeland, and
- Relevant to a law enforcement mission, including but not limited to:
    - Information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counter terrorism investigation;
    - An assessment of or response to criminal threats and vulnerabilities;
    - The existence, organization, capabilities, plans, intention, vulnerabilities, means, method, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct;
    - The existence, identification, detection, prevention, interdiction, or disruption of, or response to, criminal acts and violations of the law;

- Identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and
- Victim/witness assistance.

Mixed System has the same meaning as defined in the Department of Homeland Security's *Privacy and Civil Liberties Policy Guidance Memorandum*, Memorandum Number: 2009-01 (June 5, 2009) as any system of records that collects, maintains, or disseminates information, which is in an identifiable form, and which contains information about U.S. persons and non-U.S. persons. A "mixed system policy" is applied consistent with the Privacy Act's inapplicability to intelligence files and data systems devoted solely to foreign nationals or maintained for the purpose of intelligence activities made subject to the provisions and protections of Executive Order 12333. The mixed system policy does not establish a right of judicial review for nonresident aliens. HHS does not have a mixed systems policy. Therefore, at HHS all systems of records only contain information that meets the Privacy Act definition of being "about an individual," meaning about a citizen or permanent resident alien. Where records are commingled, only the records about citizens or permanent resident aliens are subject to the Privacy Act.

Personally Identifiable Information (PII) has the same meaning as defined in OMB Memorandum 07-16, which states, that the term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Personnel Information, for the purposes of this document, is information about HHS employees, detailees, and assignees that is collected on Office of Personnel Management standard forms 50 and 52.

Privacy Impact Assessment (PIA) has the same meaning as that term is defined in OMB Memorandum 03-22, "an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks."

Protected Information has the same meaning as that term is defined in the ISE Privacy Guidelines, Secs. (1)(b) and (13)(a)(i), which defined the term as information about U.S. citizens and lawful permanent residents that is subject to information privacy or other legal protections under the U.S. Constitution and federal laws of the United States. Protected information to be made available in the ISE includes only that which is homeland security information, law enforcement information, and terrorism information, including weapons of mass destruction information.

Record has the same meaning as the at 5 USC § 552a(a)(4), "any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph."

Routine Use has the same meaning as at 5 USC § 552a(a)(4), "any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph."

System of Records has the same meaning as at 5 USC § 552a(a)(5), "a group of any records under the control of any 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."

Terrorism Information has the same meaning as at 6 USC § 485(a)(5), which states,

The term "terrorism information"—

(A) means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to—

> (i) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;
>
> (ii) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;
>
> (iii) communications of or by such groups or individuals; or
>
> (iv) groups or individuals reasonably believed to be assisting or associated with such groups or individuals; and

(B) includes weapons of mass destruction information.

Terrorism-Related Information is information that is Terrorism Information, Homeland Security Information, or Law Enforcement Information. See Guideline 2 Report: Departments and Agencies and State, Local, and Tribal Governments, Law Enforcement Agencies, and the Private Sector (on Guideline 2 of Presidential Memorandum "Guidelines and Requirements in Support of the Information Sharing

Environment," issued December 16, 2005).**Weapons of Mass Destruction Information** has the same meaning as at 6 USC § 485(a)(6), "information that could reasonably be expected to assist in the development, proliferation, or use of a weapon of mass destruction (including a chemical, biological, radiological, or nuclear weapon) that could be used by a terrorist or a terrorist organization against the United States, including information about the location of any stockpile of nuclear materials that could be exploited for use in such a weapon that could be used by a terrorist or a terrorist organization against the United States."

X. Authorities

A. General Federal Authorities

The E-Government Act of 2002, Pub.L. 107-347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803 (December 17, 2002),

Executive Order 12333, United States intelligence activities, 46 FR 59941, 3 CFR, 1981 Comp., p. 200 (December 4, 1981).

Executive Order 13388, Further Strengthening the Sharing of Terrorism Information To Protect Americans, 70 FR 62023 (October 25, 2005).

Federal Information Security Management Act of 2002 (FISMA), 44 USC § 3541, enacted as Title III of the E-Government Act of 2002 (December 17, 2002).

Freedom of Information Act, 5 USC § 552 (July 4, 1966).

Health Insurance Reform: Security Standards; Final Rule ("The HIPAA Security Rule"), 68 FR 8334 (February 20, 2003).

Guideline 2 Report: Departments and Agencies and State, Local, and Tribal Governments, Law Enforcement Agencies, and the Private Sector (on Guideline 2 of Presidential Memorandum "Guidelines and Requirements in Support of the Information Sharing Environment," issued December 16, 2005).

Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment. Information Sharing Environment (December 4, 2006).

Standards for Privacy of Individually Identifiable Health Information; Final Rule ("The HIPAA Privacy Rule"). 65 FR 82462 (December 28, 2000).

Implementing Recommendations of the 9/11 Commission Act of 2007, Pub.L. 110–53 (August 3, 2007).

Information Sharing Environment (ISE) Functional Standard (FS), Suspicious Activity Reporting (SAR), version 1.5. ISE-FS 200 (2009).

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), *as amended* (50 USC § 402 *et seq*.) (December 17, 2004).

National Strategy for Information Sharing and Safeguarding (NSISS),Office of the President of the United States (December 2012).

OMB Circular A-130, Management of Federal Information Resources (November 28, 2000).

OMB Final Guidance on Interpreting the Provisions of the Computer Matching and Privacy Protection Act of 1988, 54 FR 25818 (June 19, 1989).

OMB Memorandum 03-22 (M-03-22), Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (September 26, 2003).

OMB Memorandum 05-08 (M-05-08), Designation of Senior Agency Officials for Privacy (February 11, 2005).

OMB Memorandum 07-16 (M-07-16), Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007).

OMB Memorandum 10-22 (M-10-22), Guidance for Online Use of Web Measurement and Customization Technologies (June 25, 2010).

OMB Memorandum 10-23 (M-10-23), Guidance for Agency Use of Third-Party Websites and Applications (June 25, 2010).

OMB Guidance on Inter-Agency Sharing of Personal Data: Protecting Personal Privacy (December 20, 2000).

OMB Privacy Act Implementation Guidelines and Responsibilities (July 9, 1975).

Presidential Memorandum "Guidelines and Requirements in Support of the Information Sharing Environment" (December 16, 2005).

Privacy Act of 1974, as amended . (Pub.L. 93-579, 88 Stat.1896, 5 USC § 552a (December 31, 1974).

Privacy and Civil Liberties Policy Guidance Memorandum, Memorandum Number: 2009-01. Department of Homeland Security (June 5, 2009).

OMB Memorandum 05-08 (M-05-08), Designation of Senior Agency Officials for Privacy (February 11, 2005).

B. HHS Authorities

HHS Policy for IT Security and Privacy Incident Reporting and Response (April 5, 2010).

HHS Office of the Chief Information Officer (OCIO) Policy for Information Systems Security and Privacy (July 7, 2011).

HHS Office of the Chief Information Officer (OCIO) Handbook for Information Systems Security and Privacy (July 7, 2011).

HHS Policy for the Information Sharing Environment (ISE) (December 2012).

HHS Policy for Privacy Impact Assessments (PIA) (February 9, 2009).

HHS Policy for Responding to Breaches of Personally Identifiable Information (PII) (November 17, 2008).

HHS Policy for Records Management (January 30, 2008).

HHS Policy for IT Policy Development (November 28, 2006).

Privacy Incident Response Team (PIRT) Charter (January 6, 2011).

HHS Privacy Act Regulations (45 CFR 5b).

XI. Acronyms

CFR	**Code of Federal Regulations**
ACL	Access Control List
CIO	Chief Information Officer
CISO	Chief Information Security Officer
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
FOIA	Freedom of Information Act
GAO	General Accounting Office
HHS	Department of Health and Human Services
IS2P	Policy for Information Systems Security and Privacy
IRTPA	Intelligence Reform and Terrorism Prevention Act
ISE	Information Sharing Environment
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
OpDiv	Operating Division
OSSI	Office of Security and Strategic Information
P-AT	Policy-Awareness and Training
P-AU	Policy-Audit and Accountability
P-PM	Policy-Performance Measurement
P-PRIV	Policy-General Privacy
PIA	Privacy Impact Assessment
PI	Protected Information
PII	Personally Identifiable Information
PIRT	Privacy Incident Response Team
PRA	Paperwork Reduction Act
RFP	Request for Proposal
SAOP	Senior Agency Official for Privacy
SDLC	System Development Life Cycle
SOP	Senior Official for Privacy
SORN	System of Records Notice
SOW	Statement of Work
SP	Special Publication
StaffDiv	Staff Division
U.S.	United States
USC	United States Code