Office of the Chief Information Officer (OCIO)
Office of the Assistant Secretary for Resources and Technology
Department of Health and Human Services (HHS)

Policy for Responding to Breaches of Personally Identifiable Information (PII)

April 15, 2008

Project:	HHS OCIO Policy
Document Number:	HHS-OCIO-2008-0001.002

Table of Contents

1. Purpose

This policy establishes the Department of Health and Human Services (HHS) Personally Identifiable Information (PII) Breach Response Team (BRT) (henceforth called the HHS BRT). It also establishes the actions to take in identifying, managing, and responding to suspected or confirmed breaches of PII.

This policy is first issuance and is issued under the authority of the HHS-OCIO-2007-0002, *Policy for Department-wide Information Security*, dated September 25, 2007.

2. Background

HHS is responsible for managing the information it stores, processes, and transmits in support of its business functions in accordance with Federal laws and regulations. Any unauthorized use, disclosure, or loss of such information can result in the loss of the public's trust and confidence in the Department's ability to properly protect it. Some information or data types, such as PII, require additional protection due to its sensitivity and the risks of misuse associated with a potential unauthorized disclosure. PII data breaches may have far-reaching implications for the individuals whose PII is compromised, including identity theft resulting in financial loss and/or personal hardship experienced by the individual. A PII data breach may also require significant HHS staff, time, assets and financial resources to mitigate, which may prevent the Department from allocating those resources elsewhere.

The *HHS Policy for Responding to Breaches of PII* ensures that responses to PII data breaches are consistent, comprehensive, complete, and delivered in an effective and timely manner that minimize risk to the Department and individuals.

3. Scope

This policy applies to all HHS organizational components (i.e., Operating Divisions, or OPDIVs, and Staffing Divisions, or STAFFDIVs) and organizations conducting business for and on behalf of the Department through contractual relationships when using HHS IT resources. This policy does not supersede any other applicable law or higher level agency directive, or existing labor management agreement in effect as of the effective date of this policy.

Agency officials shall apply this policy to employees, contractor personnel, interns, and other non-government employees. All organizations collecting or maintaining information or using or operating information systems on behalf of the Department are also subject to the stipulations of this policy. The content of and compliance with this policy shall be incorporated into applicable contract language or memoranda of agreement under separate cover, e.g., Interim HHSAR FISMA policy. Agencies shall use this policy or may create a more restrictive

OPDIV/STAFFDIV policy but not one that is less restrictive, less comprehensive, or less compliant with this Department policy.

4. Policy

The Department is responsible for the security of the information that the public has entrusted to it including PII, which can be used to distinguish or trace an individual's identity such as a name or social security number (SSN). HHS is therefore responsible for mitigating the risks associated with the inadvertent loss or unapproved disclosure of PII. In compliance with the September 20, 2006, Office of Management and Budget (OMB) Memorandum *Recommendations for Identity Theft Related Data Breach Notification*, and the May 22, 2007, OMB Memorandum (M) 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* HHS has established a breach response team. The HHS BRT is comprised of Department senior leadership representatives who engage in risk analysis to determine whether a potential or confirmed breach of PII poses problems related to identity theft or any applicable Federal law or policy. If so, the HHS BRT assesses the level of such risk and tailors the Department's response. The HHS BRT will coordinate its response with OPDIV/STAFFDIV breach analysis and incident response capabilities. This policy defines the HHS roles and responsibilities for properly managing breaches of PII at all levels of the Department and is effective immediately upon release.

4.1 HHS BRT Establishment

4.1.1 HHS shall create a breach response team and develop processes for responding to suspected or confirmed breaches of PII.

4.2 Breach Assessment

4.2.1 HHS shall develop and employ a risk-based approach, as detailed in the HHS BRT Standard Operating Procedures (SOPs), to evaluate the appropriateness and effectiveness of PII breach response activities prior to providing any external notification.

4.2.2 The HHS BRT shall identify what, if any, action(s) will be taken, as well as relay that information to the OPDIV/STAFFDIV.

4.2.3 The HHS BRT shall determine whether there is evidence of actual harm and, if so, shall assess whether the PII is at a low, moderate, or high risk of being compromised. The HHS BRT shall use the National Institute of Standards and Technology (NIST) security standards and guidance to make this assessment as specified in OMB M-07-16.[1]

[1] See OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* Attachment 3(B)(1)(a-e).

4.2.4 The HHS Information Security and Privacy Program, the HHS BRT, and all responsible organizations—including employees and contractors—are required to provide notification as specified in the roles and responsibilities below.

4.3 Breach Response

4.3.1 The HHS BRT shall evaluate response activities to ensure implementation is commensurate with the impact to the individual, the OPDIV/STAFFDIV, and the Department, and complies with applicable law(s).

4.3.2 HHS Information Security and Privacy Program shall ensure that suspected or confirmed PII breaches of 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.

4.4 Breach Notification

4.4.1 The HHS BRT shall ensure notifications are made to the affected individuals, the HHS Records Officer and third parties such as media outlets and public and private sector agencies as appropriate, regarding lost or compromised PII. The HHS BRT shall determine appropriate responses to Congressional inquiries resulting from such loss, as necessary.

5. Roles and Responsibilities

The following sections define roles and responsibilities to implement this policy.

5.1 HHS Responsible Organizations

HHS responsible organizations include the OPDIVs and STAFFDIVs. Responsible organizations shall:

5.1.1 Report within one hour of discovery all suspected or confirmed PII data breaches in any format, i.e. electronic or paper, to the HHS Chief Information Security Officer (CISO) through the HHS Information Security and Privacy Program and include the minimum information as determined by the HHS BRT SOPs. The HHS BRT Chair may request additional information as needed;

5.1.2 The HHS Records Officer shall notify the responsible organization's Records Officer of suspected or confirmed data that has been compromised.

5.1.3 Ensure OPDIV/STAFFDIV policies are consistent with the requirements set forth in this policy;

5.1.4 Ensure continuous coordination with the HHS BRT when a suspected or confirmed breach is being mitigated;

5.1.5 Assign a point of contact (POC) to conduct coordination and communication activities between the business owner at the responsible organization, the OPDIV CISO (as appropriate), and the HHS BRT for all suspected or confirmed PII data breaches;

5.1.6 Evaluate each data breach to determine the likelihood of PII loss or PII compromise;

5.1.7 Perform a risk assessment of each suspected or confirmed PII data breach to include the following: an evaluation of the impact, planned response activities commensurate with the type of loss or compromise, and the residual risk to HHS, the responsible organization(s), and to the individual(s);

5.1.8 Provide updates to the HHS Information Security and Privacy Program and the HHS BRT as additional information is discovered, including changes in status, impact, and risk;

5.1.9 Develop a response plan with the assistance of the business owner and the OPDIV CISO, for each suspected or confirmed PII data breach and provide the response plan to the HHS BRT for review and approval. The minimum timeframe and requirements for the response plan are determined by the HHS BRT Chair with the consensus of HHS BRT members;

5.1.10 If the response plan calls for the notification of affected individuals, the HHS BRT will implement a plan for notifying those individuals without unreasonable delay upon confirmation of a breach of PII; and,

5.1.11 Provide an after-action report, which contains information as determined by the HHS BRT SOPs, for the HHS BRT to review. The HHS BRT Chair may request additional information, as needed.

5.2 All Employees and Contractors

According to the *HHS Information Resources Management Policy for Establishing an Incident Response Capability,* HHS-IRM-2000-0006, dated January 8, 2001, all employees and contractors shall "report any suspected or actual computer incidents immediately to their help desk support, OPDIV Senior Information Systems Security Officer, or other designated personnel."

It is the responsibility of all employees and contractors to notify their supervisor or security officer immediately if a PII data breach is suspected or confirmed to have occurred. Additionally, all employees and contractors are required to take the general privacy awareness

training,[2] which highlights the importance of protecting PII and reviews privacy and security violations and where to report them.

5.3 HHS Information Security and Privacy Program

The HHS Information Security and Privacy Program will support the HHS BRT as needed. The Program shall:

5.3.1 Develop the HHS BRT Charter;

5.3.2 As directed by the HHS Chief Information Security Officer (CISO), notify the United States Computer Emergency Readiness Team (US-CERT) within one hour[3] of learning about a suspected or confirmed PII data breach;

5.3.3 As directed by the HHS CISO, notify the Office of the Inspector General (OIG) when a PII data breach is suspected or confirmed to have occurred;

5.3.4 Receive, process, and track reports for all PII data breaches;

5.3.5 Report PII breaches to the HHS BRT Coordinator as this information becomes available, including but not limited to initial notifications, status updates, and after-action reports. Subsequently, the HHS BRT Coordinator shall track all operational actions to completion;

5.3.6 As directed by the HHS CISO, serve as a communications channel between the HHS BRT and OPDIVs/STAFFDIVs; and,

5.3.7 Record meeting minutes for all HHS BRT meetings.

5.4 HHS BRT

The HHS BRT is composed of Department senior management and executive leadership. The members are responsible for directing and overseeing all HHS BRT activities. Details of the HHS BRT composition and member responsibilities are further defined in the *Personally Identifiable Information (PII) Breach Response Team Charter (BRT), HHS-2008-0001.001C,* dated April 14, 2008.

To fulfill its primary responsibilities, the HHS BRT shall perform the following activities:

[2] OPDIVs are not required to use the training created by the HHS Information Security and Privacy Program. Any OPDIV created training can satisfy this requirement as well.

[3] See OMB M-06-19, *Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments*.

5.4.1 Develop a charter to define the HHS BRT as a committee of the HHS Risk Management and Financial Oversight Board (RMFOB), identify executive leadership and senior management members, and define member responsibilities;

5.4.2 Appoint the HHS Chief Information Officer (CIO), who is also the designated HHS Senior Agency Official for Privacy (SAOP),[4] as the HHS BRT Chair;

5.4.3 Appoint an HHS BRT Coordinator as the liaison to the HHS Information Security and Privacy Program, the HHS BRT, and OPDIVs/STAFFDIVs to collect additional information once the initial notification is made to the HHS Information Security and Privacy Program;

5.4.4 Evaluate PII data breaches to determine the organization responsible for managing the response;

5.4.5 Assess the responsible organization's proposed course of action and proposed notification activities and provide feedback in a timely manner;

5.4.6 Receive and review the responsible organization's PII data breach risk assessments and determine whether the response plan is adequate;

5.4.7 Specify improvements in cases where the responsible organization's response plan is deemed inadequate;

5.4.8 Identify needed improvements to HHS and responsible organization data security or breach response polices and procedures;

5.4.9 Notify and consult with the proper government entities and convey the required information;[5]

5.4.10 Monitor PII data breach response activities of the responsible organization to ensure completion;

5.4.11 Each member of the HHS BRT is responsible for notifying the necessary members of their organization of incidents to initiate internal response activities;

5.4.12 Conduct after-action reviews and monitoring activities to confirm the completion of PII data breach response activities and provide recommendations for improvement;

[4] Per OMB M-05-08, *Designation of Senior Agency Officials for Privacy,* HHS has designated the HHS CIO as the SAOP. Should this designation change, both the HHS CIO and SAOP must sit on HHS BRT, with the HHS CIO continuing to serve as HHS BRT Chair.

[5] See OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* Attachment 2(A)(1).

5.4.13 Provide notification and assessment of information breaches to RMFOB;

5.4.14 Prepare an annual report of all HHS BRT activities each calendar year and provide the report to the RMFOB, OPDIV/STAFFDIV heads, and OPDIV CIOs; and,

5.4.15 Ensure notification to the affected individuals; the HHS Records Officer; and, third parties such as media outlets and public and private sector agencies as appropriate, regarding lost or compromised PII.

6. Applicable Laws and Guidance

- Public Law 93-579, *Privacy Act of 1974,* dated December 31, 1974.
- OMB Memorandum, *Recommendations for Identity Theft Related Data Breach Notification*, September 20, 2006.[6]
- OMB Memorandum 06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, dated July 12, 2006.
- OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* dated May 22, 2007.
- *HHS Information Resources Management (IRM) Policy Circular No 101, Chief Information Officer Roles and Responsibilities,* dated March 1999.
- *HHS Information Resources Management (IRM) Policy for Establishing an Incident Response Capability,* HHS-IRM-2000-0006, dated January 8, 2001.

7. Information and Assistance

All Department policies, standards, procedures and information security controls are posted on the following website: http://www.hhs.gov/ocio/policy/index.html. Direct questions, comments, suggestions, or requests for further information to the HHS Information Security and Privacy Program at (202) 205-9581.

8. Effective Date/Implementation

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

These policies and procedures will not be implemented in any recognized bargaining unit until the union has been provided notice of the proposed changes and given an opportunity to fully exercise its representational rights.

[6] No OMB number was assigned to this memorandum.

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 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.

9. Approved

/s/ (John Teeter for) April 15, 2008

Michael W. Carleton
HHS Chief Information Officer
Designated HHS Senior Agency Official for Privacy

Date

Glossary

Breach – the compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or loss of control of personally identifiable information (PII). Any similar term referring to situations where 1) unauthorized persons or 2) authorized persons with unauthorized privileges have access or potential access to PII, physical or electronic.

Personally Identifiable Information (PII) – information in an IT system or online collection: (1) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.), or (2) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors.)

Risk – the level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, given the potential impact of a threat and the likelihood of that threat occurring.

Risk Assessment – the process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system. Part of risk management and synonymous with risk analysis, risk assessment incorporates threat and vulnerability analyses and considers mitigations provided by established or planned security controls.