DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Secretary

Washington, D C 20201

Karen Evans
Executive Office of the President
Office of Management and Budget (OMB)
Washington, DC 20503

Dear Ms. Evans,

On May 22, 2007 OMB released Memorandum (M) 07-16 entitled *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*. The Department of Health and Human Services (HHS) is pleased to provide the attached report in response to M-07-16.

Should you have any questions regarding this report, please direct them to Mark Brown, Deputy Chief Information Security Officer, at (202) 690-8685.

Sincerely,

Michael W. Carleton
Chief Information Officer (CIO)

Enclosures

Response to Attachment 1: Safeguarding Against the Breach of Personally Identifiable Information (PII)

HHS' Review of Existing Federal Privacy and Security Law and Guidance

Attachment 1 reemphasizes the responsibilities under existing laws, executive orders (E.O.) and regulations, and policies to appropriately safeguard PII, including training employees of their responsibilities. As part of the development of a breach notification policy, agencies are required to review existing requirements with respect to privacy and security. In particular:

- The Privacy Act of 1974 requires each agency to establish and implement rules of conduct; establish and maintain appropriate administrative, technical, and physical safeguards; and maintain accurate, relevant, timely, and complete information;
- Agencies must follow the processes outlined in Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, to implement minimum security requirements and controls;
- Specific to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* agencies must certify and accredit (C&A) information systems; and
- Agencies must train employees in their security and privacy responsibilities before permitting access to agency information and information systems.

HHS will review each of the aforementioned privacy and security requirements to ensure that the Department is complying with its obligations under the applicable legal requirements and that its compliance with these legal requirements on the protection of PII stored, processed, and transmitted within the agency is consistent with:

- Federal Information Security Management Act (FISMA) requirements mandated, most recently, by OMB M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*; and
- President's Management Agenda (PMA) goals.

In addition to FISMA and PMA reporting oversight and evaluation, HHS requires a Privacy Impact Assessment (PIA) for each information system. Department personnel perform annual reviews of system of records notices (SORN) to ensure that systems of records are appropriately maintained. Finally, HHS has implemented both security and privacy awareness training, and requires rules of behavior to be reviewed and signed before employees are authorized to access PII or the HHS network.

HHS Plan to Review Holdings of PII

Attachment 1 requires HHS to develop a plan to review all holdings of PII. This plan must be included as an attachment to the HHS FY07 FISMA report and must be publicly published. At HHS, routine reviews of our collections of PII are conducted on an ongoing basis, and the Department supplements these reviews with targeted attention, as necessary.

At a minimum of every three years, as required by statute, the Department incorporates a review of PII contained within Information Collection Requests (ICR) covered by the Paperwork Reduction Act (PRA). Any information collections, which must be amended, are addressed at the time of the review, as well. These reviews cover the majority of the information collected by

HHS. Most of our holdings are data collected from either online via application forms or through survey research. The goal of these reviews is to ensure compliance with Privacy Act requirements, such as the need to collect information to the greatest extent practicable from the subject individual,[1] and with the requirements of the PRA to reduce burden and ensure practical utility of the information collected.

Data collected from federal employees is not required to comply with the PRA, unless the results of the collection are to be used for statistical purposes, such as compilations of general public interest. The Office of Personnel Management (OPM) has notified all government agencies about their work to complete guidance for agencies on the reduction of social security numbers (SSNs) and the collection and maintenance of information about federal employees. Rather than duplicate OPM's efforts by creating policies that may be incorrect or inconsistent with OPM policies, HHS awaits their guidance and plans to defer to their expertise in this area. Secure One HHS will use this guidance to coordinate the completion of the tasks in Table 1.

As required by Circular A-130, Appendix I, HHS reviews a random sample of contracts that provide for the maintenance of systems of records and our recordkeeping practices biannually. Furthermore, as required by the Privacy Act of 1974, when decisions are made about individuals that affect their rights, benefits, or privileges, HHS reviews the record to make certain it is as accurate, timely, relevant, and complete as required to ensure fairness to the individual in making the decision.

Most important, HHS has undertaken other major reviews of PII outside of federally mandated annual reviews. Prior to the issuance of OMB M-07-16, HHS determined that it would be appropriate to evaluate each operating divisions (OPDIVs) holding, and have begun that review targeting the largest and most important collections of the Department. The Administration for Children and Families (ACF) maintains records on over 200 million individuals, especially in the Child Support Enforcement program, and the Centers for Medicare & Medicaid Services (CMS) holds over 42 million records, especially on Medicare beneficiaries. Since these two agencies hold, by far, the most complex PII in the Department, additional reviews have begun at these two important OPDIVs. Additionally, CMS is conducting an internal review of its systems of records under the Privacy Act, and has already begun to publish amendments to update the systems. HHS is in the process of establishing a similar review at ACF. HHS expects this contract to be in place before the end of the 2008 fiscal year. Following completion of this work at CMS and ACF, HHS will choose other OPDIVs to review and update each year. This will ensure that the systems of records are updated regularly on a rolling basis.

Finally, during the next 18 months, HHS plans to conduct a review of its holdings to determine whether there are any significant collections of PII that do not fall into one of the above categories and that may, as a result, go unnoticed during one of the Department's routine reviews. That review will be conducted jointly by the Director of the Freedom of Information/Privacy Acts Division of the Office of the Assistant Secretary for Public Affairs (ASPA) and the Senior Agency Official for Privacy, and fulfilled by the HHS CIO.

HHS' Plan to Review and Reduce the Unnecessary Use of SSNs

Attachment 1 also requires HHS to develop a plan to review the use of SSN throughout Departmental systems. HHS must identify instances in which collection or use of SSNs is

[1] 5 U.S.C. 552a(e)(2).

unnecessary, and establish a plan to eliminate the unnecessary collection and use of SSNs within 18 months of submitting the plan to OMB.

HHS continually reviews the collection of SSNs through the PRA ICR process. HHS will leverage this existing process to review ICRs that include the collection of SSNs due for extensions in Calendar Year (CY) 2008, 2009, and 2010. HHS will also inventory and review PRA-exempt uses of SSNs with specific attention to those collections related to clinical research and treatment; these have the highest probability of including use of SSNs.

HHS notes that many cases of SSN collection and use are required under the Debt Collection Improvement Act of 1996 (DCIA, P.L. 104-134, 110 STAT. 1321), which added the following provision to section 7701 of Title 31 of the United States Code:

(c)(1) The head of each Federal agency shall require each person doing business with that agency to furnish to that agency such person's taxpayer identifying number.

(2) For purposes of this subsection, a person shall be considered to be doing business with a Federal agency if the person is--

(A) a lender or servicer in a Federal guaranteed or insured loan program administered by the agency;

(B) an applicant for, or recipient of, a Federal license, permit, right-of-way, grant, or benefit payment administered by the agency or insurance administered by the agency;

(C) a contractor of the agency;

(D) assessed a fine, fee, royalty or penalty by the agency; and

(E) in a relationship with the agency that may give rise to a receivable due to that agency, such as a partner of a borrower in or a guarantor of a Federal direct or insured loan administered by the agency.[2]

This provision is extremely broad and, because the SSN constitutes the taxpayer identifying number for most individuals, the provision requires HHS to collect and maintain SSNs of almost every individual who comes into contact with the agency. HHS collects information about individuals covered by this provision in various categories, including our benefit programs, entitlement programs (such as the CMS programs), research purposes, loan programs, employees, and contractors.

By law, HHS cannot reduce the collection of SSNs in several categories unless a legislative change is made to the DCIA. In some cases, HHS collects SSNs when comparing survey or clinical data to administrative records, or when conducting a longitudinal study, which requires follow-up to keep track of where individuals may reside. With these cases, it is possible HHS may be able to use other approaches that would not require the collection of SSNs. As opportunities arise, HHS plans to engage in government sanctioned meetings regarding alternative means to reduce the use of SSNs as a personal identifier. Therefore, HHS will review the circumstances under which the agency uses SSNs to identify studies that may not need them. HHS will review the use of SSNs according to the schedule found in Table 1.

[2] For the full text of the Debt Collection Improvement Act of 1996, please reference Public Law 104-134, 110 STAT. 1321.

Table 1. SSN Review Plan Schedule[3]

Task	Date Start	Date Complete	Activity
Inventory all PRA ICRs for Use of SSN	10/1/2007	10/31/2007	ICRs will be categorized for review into those that are mandatory (e.g under the DCIA) and those that are discretionary (e.g. longitudinal studies)
Inventory all PRA ICRs to Categorize whether Mandatory or Discretionary Use of SSN	10/1/2007	10/31/2007	Of specific concern is exemption #5 for clinical research, treatment, etc.
Review guidance as issued by OPM to determine consitancy in the collection and use of federal employee SSN	10/1/2007	10/31/2007	Incorporate OPM guidance into HHS guidance
Develop Guidance for Review of SSN Use	10/1/2007	11/23/2007	Guidance will be issued to OPDIV PRA staff and OS PRA Desk Officers
Schedule all 2009-2010 expiring ICRs for SSN Review	11/1/2007	11/23/2007	Conduct internal interviews with PRA contacts and privacy stakeholders to review unnecessary use of SSNs and ensure that guidance is fully understood
Review PRA exempt use of SSN (non-federal employee)	1/2/2008	12/31/2008	Work with PRA and Privacy Act contacts to determine acceptable uses of SSN
Review 2008 Expiring ICRs for Use of SSN	1/2/2008	12/31/2008	2008 Expiring ICRs will be reviewed as they come up for extension on regular schedule

HHS Status of Implementing OMB M-06-16 Controls

Finally, Attachment 1 discusses five security requirements that HHS must implement, derived from existing security policy and NIST guidance.[4] These five security requirements require HHS to:

- **Encrypt**, using only NIST certified cryptographic modules, all data on mobile computers/devices carrying agency data;
- **Allow remote access** only with two-factor authentication;
- **Use a time-out** function for remote access and mobile devices requiring user re-authentication;
- **Log all computer-readable data** extracts from databases holding sensitive information; and

[3] Within eighteen months of submission to the Office of Management and Budget (OMB), the Department must conduct these activities. As the schedule progresses, HHS will release guidance to clarify the activities

[4] For specific guidance and references related to these security activities, please reference OMB M-06-16, *Protection of Sensitive Agency Information.*

- **Ensure all individuals** with authorized access to PII and their supervisors sign, at least annually, a document clearly describing their responsibilities.

In response to these requirements, HHS has developed and implemented the following:

Table 2. OMB M-06-16 Security Control Review

Security Requirement	Status	Documentation
Implement NIST certified encryption on all mobile computers/devices	In progress (above 90% compliance)	Internal Draft HHS Memorandum ISP-2007-001 Internal HHS Memorandum ISP-2007-002 Internal Draft HHS Memorandum ISP-2007-006
Allow remote access only with two-factor authentication	Activities are being aligned with Personal Identity Verification (PIV) implementation as part of Homeland Security Presidential Directive (HSPD) 12 implementation	N/A
Implement a 30-minute time-out for remote access and all mobile devices	A policy has been drafted and is currently under review. The Federal Desktop Core Configuration (FDCC) specify a more stringent 15-minute time out which meets this requirement. This security setting is mandated to be in place by February 1, 2008	Internal Draft Memorandum ISP-2006-006 Internal Draft Memorandum ISP-2006-009 FDCC Documentation Release 1.0 Office of Mangement and Budget (OMB) Memoranda 07-11, *Implementaiton of Commonly Accepted Security Configurations for Windows Operating Systems*
Log and verify all computer-readable data extracts, and ensure erasure within 90 days, if data is no longer needed	Currently this requirement is being reviewed by HHS to determine an efficient way to incorporate it until information assurance practices. HHS is monitoring other federal agencies to determine options for incorporating this security control	N/A
Ensure employees and supervisors understand their responsibilities regarding access to PII	Complete	HHS Security Awareness Training HHS General Privacy Awareness Training HHS Security Role-based Training HHS Senior Official for Privacy Role-based Training

Response to Attachment 2: Incident Reporting and Handling Requirements

HHS' Plan to Implement Incident Management Guidance

Attachment 2 provides HHS with incident management guidance for incidents involving the breach of PII. Following NIST and FIPS guidance,[5] and the President's Identity Theft Task Force recommendations, HHS has updated its Incident Management Policy to reflect this guidance. A draft copy of HHS' Incident Management Policy will be provided upon OMB's request.

HHS' Plan to Incorporate Routine Use Language Guidance

Department staff have carefully reviewed the recommended routine use language, specifically the language governing disclosures in the event of data breaches, and determined that such language may not be effective in HHS. The language is vague and may not be an effective guide for agency staff. Following our review, HHS proposes the more tailored routine use language below:

> To appropriate federal agencies and Department contractors that have a need to know the information for the purpose of assisting the Department's efforts to respond to a suspected or confirmed breach of the security or confidentiality of information maintained in this system of records, and the information disclosed is relevant and necessary for that assistance.

HHS staff identified four types of recipients to whom disclosures may need to be made in the case of a security incident: law enforcement, contractors, the Department of Homeland Security (DHS) United States Computer Emergency Readiness Team (US-CERT), and agency program partners. In the case of disclosures to law enforcement, almost every HHS system of records has a routine use clause intended to cover situations in which information about a potential violation of law is discovered. It is broad enough to cover federal, state, local, tribal, and foreign entities, and addresses criminal, civil, regulatory, and administrative law enforcement functions. As such, there exists no need for updated routine use language for situations involving the disclosure of information to these recipients.

In the case of HHS contractors, most HHS systems of records incorporate routine use language to disclose PII to contractors carrying out a mission on behalf of the agency. As the language may not be broad enough to encompass incident response duties, HHS has accommodated this consideration in our tailored language above.

HHS is required to report incidents to US-CERT. This type of report includes information such as the system(s) involved, the categories and number of individuals whose records are at risk, the types of data potentially disclosed, whether or not SSNs are included, and the circumstances surrounding the incident. A routine use clause permits the disclosure of individually identifiable data. Since HHS does not disclose individually identifiable data to US-CERT, routine use language is not required for that purpose.

Finally, HHS has data use agreements with other agencies with which they share information as it is possible that an incident could involve HHS data while in the custody of another agency, or

[5] For additional information regarding the National Institutes of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) publications and 800 series Special Publications, please see www.nist.gov.

another agency's data in HHS' custody. In those circumstances, HHS will share individually identifiable data with the other agency partner, and the tailored language accommodates this potential need.

All new systems of records will include the tailored language where there is no statutory or policy reason to exclude it. In addition, in our methodical review of systems of records, as they are amended, updated, or revised, HHS will take the opportunity to add the above routine use language at that time.

Response to Attachment 3: External Breach Notification

HHS' Plan to Develop and Implement a Breach Notification Policy

Attachment 3 provides a framework for HHS to consider when determining the appropriate PII breach notification to members of the public. As part of HHS' approach to overall breach response management, recommendations found in Attachment 3 will be incorporated into its *HHS PII Breach Response Team Policy*. The *HHS PII Breach Response Team Policy* is attached to this report. In addition, the Breach Response Team is drafting *HHS PII Breach Response Team Standard Operating Procedures*. Recommendations for external breach notification management will be incorporated into these formal procedures. Once complete, these procedures will support implementation of the *HHS PII Breach Response Team Policy*.

Response to Attachment 4: Rules and Consequences

HHS' Plan to Develop and Implement 'Rules and Consequences' Guidance

Attachment 4 requires HHS to develop and implement a policy outlining and identifying consequences and corrective actions available for failure to follow HHS' rules of behavior, consistent with the law and any applicable collective bargaining agreement. HHS has incorporated recommendations provided in Attachment 4 into the *Information Security Rules of Behavior*. The *Information Security Rules of Behavior* provides a comprehensive description of responsibilities for safeguarding PII and establishes common rules on the appropriate use of all HHS information technology (IT) resources.