





Information Security Program

Machine-Readable Privacy Policy Guide

July 19, 2005

SECURE ONE HHS

KEEP AMERICA'S HEALTH AND HUMAN SERVICES SECURE

Table of Contents

Preface

As the Department of Health and Human Services (HHS) Information Technology Security Program evolves, this document will be subject to review and update, which will occur annually or when changes occur that signal the need to revise the *HHS Machine-Readable Privacy Policy Guide*. These changes may include the following:

- Changes in roles and responsibilities;
- Release of new executive, legislative, technical, or Departmental guidance;
- Identification of changes in governing policies;
- Changes in vulnerabilities, risks or threats; and/or
- HHS Inspector General findings that stem from a security audit.

The HHS Chief Security Officer (CSO) must approve all revisions to the *HHS Machine-Readable Privacy Policy Guide*. Revisions are to be highlighted in the Document Change History table. Each revised guidance document is subject to HHS' document review and approval process before becoming final. When it is approved, a new version of the *HHS Machine-Readable Privacy Policy Guide* will be issued, and all affected parties will be informed of the changes made.

Additionally, compliance with this document is voluntary, but highly recommended as it contains best practices for integrating privacy into the information security program.

Document Change History

Version Number	Release Date	Summary of Changes	Section Number/Paragraph Number	Changes Made By
1.0	02/07/2005	Initial Draft Release	N/A	N/A
2.0	04/06/2005	Final Document Release	N/A	N/A
3.0	07/19/2005	Updated to reflect new HHS guidance and regulatory requirements.	Throughout	HHS CSO

1.Introduction

HHS is required under Section 208 of the E-Government Act of 2002 "to translate privacy policies into a standardized machine-readable format."[1] In its guidance accompanying Section 208, the Office of Management and Budget (OMB) further defined the requirement that agencies "adopt machine-readable technology that alerts users automatically about whether site privacy practices match their personal privacy preferences. Such technology enables users to make an informed choice about whether to conduct business with that site."[2]

1.1 Purpose

This guide outlines a standard approach for implementing a machine-readable privacy policy on HHS public websites. It provides a standard Machine-Readable Data Analysis Worksheet and detailed instructions for filling out the worksheet. Completing the analysis worksheet is not a requirement, however, it will assist in creating an accurate machine-readable privacy policy. This guide also provides a summary of federal legislative, regulatory, and guidance requirements related to website privacy practices.

All HHS public websites must have machine-readable privacy policies by June 15, 2005.

1.2 Background

The federal government has recognized the publics increasing online privacy concerns. Individuals are concerned with what information is collected on websites, how it is used, and whether or not they have a choice in providing the information. By providing this guide, HHS also recognizes the publics growing demand that website information collection practices and use become increasingly transparent and are compliant with all related privacy legislation, regulation, and guidance.

With an estimated online presence of more than 10 million Web pages, it is critical that HHS follow federal privacy guidelines. Public citizens, private sector, and public sector organizations interacting with HHS must be informed of website privacy practices on the following:

- Choices—options users have on using their voluntary and mandatory collected data (opt-in or opt-out)
- Access—who has access to data and if customers can access or correct their own data

1 *E-Government Act of 2002*, Section 208(C)(2).
2 OMB Memorandum 03-22, *Implementing the Privacy Provisions of the* E-Government Act of 2002, Attachment A, Section IV.

- Usage—for what business purpose collected data is used and disclosed
- Sharing—with whom data is shared and why and whether sharing is optional
- Expiration—how long information is retained.

1.3 Scope

All HHS websites should have a machine-readable privacy policy on all public websites to ensure compliance with the E-Government Act of 2002. Machine-readable privacy policies are not required on HHS Intranet websites. This guide applies to all HHS personnel, which includes the Operating Divisions (OPDIV) and contractors responsible for managing and operating public websites on behalf of HHS or OPDIVs.

This guide will familiarize HHS personnel with machine-readable privacy requirements set forth in the E-Government Act of 2002 and machine-readable privacy specification, Platform for Privacy Preferences (P3P), developed by the World Wide Web Consortium (W3C).

1.4 Document Organization

The remainder of the document is structured as follows:

- Section 1 describes federal privacy requirements.
- Section 2 provides roles and responsibilities during the implementation process.
- Section 3 describes the process of implementing a machine-readable privacy policy.
- Section 4 provides step by step guidance on how to develop and implement a machine-readable privacy policy.
- Section 5 provides a conclusion summarizing the points of this guide.

This guide also contains the following appendices:

- Appendix A provides a feedback form for use in submitting comments on this document to HHS.
- Appendix B lists the acronyms used in this document.
- Appendix C defines terms most frequently used in this document.
- Appendix D lists references for this document.
- Appendix E provides the Machine-Readable Data Analysis Worksheet.
- Appendix F provides a list of all documents associated with the HHS Information Security Program.

2. Federal Privacy Requirements

Privacy and an agency's online presence are closely interrelated and are a source of great concern for IT managers, system owners, and members of the public. The legislative and regulatory requirements and guidance summarized in this section reflect the evolving federal approach of integrating privacy requirements into overall IT security programs and plans and website requirements.

2.1 Federal Statutes

Public laws require federal agencies to disclose website information collection and use practices to protect the privacy of individuals visiting their websites. Applicable statutes, including major legislation, such as the E-Government Act of 2002 and the Privacy Act of 1974, are described below.

The material in this guide is consistent with federal laws and guidance existing at the time it was drafted. It will be updated as federal legislation and regulations change or are made available.

2.1.1 The Privacy Act of 1974

The Privacy Act of 1974 protects the privacy of individuals by establishing "Fair Information Practices" for the collection, maintenance, use, and dissemination of information by federal agencies. For several years the Privacy Act, along with its accompanying case law, was the most significant milestone in the history of the protection of the privacy of personal information held by the federal government. In the more recent past, subsequent laws, regulations, and guidance have built upon the principles first articulated in the Privacy Act.

2.1.2 The E-Government Act of 2002

Title II of the E-Government Act of 2002, Section 208, requires federal agencies to conduct privacy impact assessments (PIA) prior to developing or procuring information technology (IT) systems that collect, maintain, or disseminate information in identifiable form (IIF). Once completed, the OPDIV Chief Information Officer (CIO), or an equivalent official, must review the PIAs and submit them to HHS' Office of Information Resources Management (OIRM) to be made publicly available at http://www.hhs.gov/pia.

Title II identifies website privacy policy requirements. Federal agencies must include a machine-readable privacy policy on agency websites the public uses. Also, federal agencies' privacy policy notices must be consistent with the privacy policy requirements outlined in Section 552a of the Privacy Act of 1974. Privacy notices must address the following:

- What information is to be collected;

- Why the information is being collected;
- The intended use of the agency of the information;
- With whom the information will be shared;
- What notice or opportunities for consent would be provided to individuals on what information is collected and how that information is shared;
- How the information will be secured; and
- The rights of the individual under Section 552a of title 5, United States Code (commonly referred to as the "Privacy Act"), and other laws relevant to the protection of the privacy of an individual.

In addition, Section 207 requires federal agencies to develop priorities and schedules for making government information available and accessible to the public and report to OMB as part of the agency's annual E-Government Act report.

2.1.3 The Children's Online Privacy Protection Act of 1998

The Children's Online Privacy Protection Act (COPPA) of 1998 applies to private sector websites that collect personal information online from children under the age of 13. OMB Memorandum 00-13, Privacy Policies and Data Collection on Federal Websites, extended the provisions of COPPA to federal websites. COPPA identifies the content that a website operator must include in a privacy policy, outlines when and how to seek verifiable consent from a parent, and specifies the responsibilities an operator has for protecting children's privacy and safety online.

Further discussion of COPPA requirements, compliance, and implementation can be found in the Federal Trade Commission's COPPA website at http://www.ftc.gov/bcp/conline/edcams/coppa/ intro.htm.

2.1.4 The Clinger-Cohen Act of 1996

The Clinger-Cohen Act of 1996 (which includes both the Information Technology Management Reform Act and the Federal Acquisition Reform Act) is intended to improve the productivity, efficiency, and effectiveness of federal programs through the improved acquisition, use, and disposal of IT resources. Among other effects, it makes agencies responsible for IT resource acquisition and management, under the guidance of the CIO, and emphasizes that value must be maximized and risk minimized in the capital planning and budget processes. In effect, the Clinger-Cohen Act places the burden of incorporating privacy controls into IT investments at the agency and CIO levels.

2.1.5 The Health Insurance Portability and Accountability Act of 1996

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 affects the health insurance industry and contains provisions under the heading of "Administrative Simplification" that govern how health care institutions, in both the government and private sectors, handle protected health information (PHI), a subset of IIF. Regulations published in 2000, pursuant to these provisions, establish

standards for providing notice of how health information collected from users of a covered entity's services will be used and disclosed, and they grant certain rights to individuals, including the right to see one's health records and to request corrections or other amendments to those records. These regulations apply to both written and oral PHI.

Further discussion of HIPAA requirements, compliance, and implementation can be found in the HHS HIPAA Compliance Guide and the HHS Office of Civil Rights (OCR) HIPAA Privacy Web page at http://www.hhs.gov/ocr/hipaa/.

2.1.6 The Paperwork Reduction Act of 1995

The Paperwork Reduction Act (PRA) focuses on the timely, equitable, efficient, and appropriate manner of information dissemination to the public. The PRA specifies that among their other responsibilities, CIOs shall improve protections for the privacy and security of information under their agencies' control. The PRA also created the Office of Information and Regulatory Affairs within OMB to provide central oversight of information management activities across the federal government. The PRA also requires agencies to receive an OMB information collection approval number, a.k.a. an "OMB control number," for an information system prior to using that system to collect information from any person.

2.1.7 The Computer Matching and Privacy Protection Act of 1988

The Computer Matching and Privacy Protection Act of 1988 added several new provisions to the Privacy Act of 1974. "Computer matching" occurs when federal and/or state agencies share IIF. Agencies use computer matching to conduct many government functions, including establishing or verifying eligibility for federal benefit programs or identifying payments or debts individuals owe to government agencies.

The Computer Matching and Privacy Protection Act requires agencies engaged in computer matching activities to:

- Provide individuals notice if their IIF is being computer matched;
- Allow individuals opportunity to refute adverse information before having a benefit denied or terminated; and
- Establish Data Integrity Boards to oversee computer-matching activities.

2.1.8 The Freedom of Information Act of 1966

The Freedom of Information Act (FOIA) of 1966 requires all agencies of the executive branch to disclose federal agency records or information upon receiving a written request for them from any individual, except for those records or portions of them that are protected from disclosure by certain exemptions and exclusions.

2.1.9 The Federal Data Quality Act

Section 515 of the Treasury and General Government Appropriations Act for Fiscal Year 2001, informally known as the Federal Data Quality Act or Information Quality Act, outlines the quality of information disseminated by federal agencies. Section 515 required OMB to develop government-wide standards to ensure the quality, objectivity, utility, and integrity of information disseminated by federal agencies. OMB issued final government-wide guidelines in the Federal Register Vol. 67, No. 36.

2.2 Federal Memoranda and Other Guidance

HHS must also comply with OMB guidance on implementing these various legislative acts. This section lists some important, but by no means exhaustive, list of OMB memoranda regarding privacy and information resource management.

2.2.1 Federal Register Vol. 67, No. 36

OMB issued the Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies Republication as the final guidelines for implementing Section 515 of the Treasury and General Government Appropriations Act for Fiscal Year 2001. Under these guidelines, federal agencies are directed to develop information resources management procedures for reviewing and substantiating the quality, objectivity, utility, and integrity of information before it is disseminated.

In addition to complying with the guidelines, federal agencies must issue their own information quality guidelines and establish administrative mechanisms allowing affected persons to seek and obtain correction of information maintained and disseminated by the agency that does not comply with these OMB guidelines.

2.2.2 OMB Memorandum M-05-04

OMB has provided federal agencies with Memorandum (M) 05-04, Policies for Federal Agency Public websites, under the requirements of Section 207 of the E-Government Act of 2002.
OMB M-05-04 reiterates federal agencies' responsibilities under existing information resource management law and guidance and establishes several new requirements. New requirements include the following:

- Establishing and maintaining information dissemination product inventories, priorities, and schedules;
- Establishing and enforcing agency-side linking policies;
- Assuring agencies principal and public website and any other major entry point include a search function; and
- Using approved domains only (.gov, .mil, or fed.us) for the sponsorship of an information dissemination products, including public websites.

2.2.3 OMB Circular A-130, Appendix III

OMB Circular A-130, Management of Federal Information Resources, outlines requirements in Appendix I and III. Appendix III requires agencies to implement security requirements for, and to protect personal information in, automated information systems. Appendix III provides specific guidelines for implementing these requirements, including a minimum set of controls for federal automated information programs. Appendix III also assigns federal agency responsibilities for the security of automated information and links agency automated information security programs and agency management control systems established in accordance with OMB Circular A-123, Management Accountability and Control. OMB A-130 requires agencies to adopt three types of privacy and security controls:

- **Assigning Responsibility for Security.** Responsibility for the security of IT systems must be assigned to a person with the appropriate qualifications, ability, and authority to provide security.
- **Planning for Security**. System security plans should be incorporated into the organization's information resource management planning process, consistent with guidance issued by the National Institute of Standards and Technology (NIST).
- **Reviewing Security Controls.** Agencies must review security controls whenever significant modifications are made, no less than once every three years. The scope and frequency of the review should be commensurate with the acceptable level of risk. It is important to consider whether personal information is contained in the system when assessing risk.

2.2.4 OMB Circular A-11

OMB Circular A-11, Preparation, Submission, and Execution of the Budget, provides guidance to federal agencies on preparing and submitting budget estimates to the OMB. Section 31.8 of Circular A-11 requires that agency estimates should "reflect a comprehensive understanding of OMB security policies and NIST guidance." This understanding needs to be supported by the following measures:

- Identifying additional security controls for systems that promote or permit public access, other externally accessible systems, and those that are interconnected with systems over which program officials have little or no control;
- Demonstrating how the agency ensures the effective use of security controls and authentication tools to protect privacy for those systems that promote or permit public access; and
- Demonstrating how the agency ensures that handing personal information is consistent with relevant government-wide and agency processes.

2.2.5 OMB Memorandum M-03-22

OMB has provided federal agencies with M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 2003. This guidance directs agencies to conduct reviews of how they use technology to collect new information and when they buy or develop new IT systems to handle collecting IIF as well as website privacy policy content.

M-03-22 indicates that PIAs should be conducted if any of the following nine circumstances occur:

- **Conversions.** When converting paper-based methods to electronic systems.
- **Anonymous to Non-Anonymous.** When the system's function, as applied to an existing information collection, changes anonymous information into IIF.
- **Significant System Management Changes.** When new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system.
- **Significant Merging.** When agencies adopt or alter business processes so that government databases holding IIF are merged, centralized, matched with other databases, or otherwise significantly manipulated.
- **New Public Access.** When user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system that members of the public can access.
- **Commercial Sources.** When agencies systematically incorporate into existing information systems databases of IIF purchased or obtained from commercial or public sources.
- **New Interagency Uses.** When agencies work together on shared functions involving significant new uses or exchanges of IIF.
- **Internal Flow or Collection.** When alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional IIF.
- **Alteration in Character of Data.** When new IIF added to a collection raises the risks to personal privacy, such as the addition of health or privacy information.

In addition to the PIA requirements, M-03-22 outlines new and previously established requirements for privacy policies on agency websites. New content requirements outlined in M-03-22 include ensuring website privacy policies inform website visitors of their rights under the Privacy Act or other applicable privacy laws and implementing machine-readable privacy policies on all public websites.

2.2.6 OMB Memorandum 01-05

OMB M-01-05 provides guidance on implementing the Computer Matching and Privacy Protection Act of 1988. M-01-05 states that agencies must "prior to any data sharing...review and meet the Privacy Act requirements for computer matching, including developing a computer matching agreement and publishing notice of the

proposed match in the Federal Register." The memorandum then states that it "puts forth principles on protecting personal privacy when conducting inter-agency data sharing," including:

- Notice
- Consent, as appropriate
- Re-disclosure limitations
- Accuracy
- Security controls

While Memorandum 01-05 stresses these privacy protections, it also discusses additional privacy protections in a section entitled "Other Guidance." These additional privacy protections are:

- Employing the principle of minimization
- Employing the principle of accountability
- Conducting PIAs

2.2.7 OMB Memorandum 99-18

OMB M-99-18, Privacy Policies on Federal Websites, directs federal agencies to post privacy policies on principle websites, major entry points, and websites in which substantial personal information is collected from the public. Agency privacy policies must clearly and concisely inform visitors to the site what information the agency collects about individuals, why the agency collects it, and how the agency will use the information.

2.2.8 OMB Memorandum 00-13

OMB M-00-13, Privacy Policies and Data Collection on Federal Websites, reiterates website privacy policy requirements and issues guidance prohibiting the use of cookies on federal agency websites. OMB later updated the guidance issued in M-00-13 to prohibit only the use of persistent cookies. Unless the agency demonstrates a compelling need for the persistent cookie, its use is approved by the agency head. The prohibition of persistent cookies does not include using session cookies.

3.Machine-Readable Privacy Policy Roles and Responsibilities

Federal guidance on implementing a machine-readable privacy policy assigns specific responsibilities to the HHS Department leadership. Other staff, however, may have responsibilities for developing or implementing the machine-readable privacy policy or providing information relevant to its completion.

3.1 Headquarters Level

Developing and implementing a machine-readable privacy policy at the headquarters (HQ) level ensures that HHS websites comply with relevant privacy laws and policies. The following leadership roles have specific responsibilities related to implementing a machine-readable privacy policy.

3.1.1 HHS CIO

The HHS CIO is responsible for:

- Designating responsibility for oversight of the machine-readable privacy policy implementation process at OPDIV level to the OPDIV CIO.

3.1.2 HHS Chief Security Officer (CSO)

The HHS CSO is responsible for:

- Providing a standard methodology and requirements for developing and implementing machine-readable privacy policy;
- Reporting annually to OMB on compliance with Section 208 of the E-Government Act; and
- Coordinating and analyzing the machine-readable privacy policy implementation process to identify improvements.

3.1.3 HHS Web Management Team

The HHS Web Management Team is responsible for:

- Working with the HHS CSO, HHS Privacy Act Officer, and the HHS Privacy Advocate to ensure that proper machine-readable privacy policies are published on web servers managed by the Office of the Secretary.

3.1.4 HHS Privacy Advocate

The HHS privacy advocate is responsible for:

- Serving as a resource for privacy programs and awareness;
- Serving as Chairman of the HHS Data Council Privacy Subcommittee;
- Encouraging awareness of potential privacy issues and policies;
- Accessing policy process to review regulations, legislative proposals, etc.;
- Providing privacy-related guidance as needed; and
- Serving as a liaison to external organizations.

3.1.5 HHS Privacy Act Officer

The HHS Privacy Act Officer is responsible for:

- Focusing on applicable case law;
- Reviewing HHS Privacy Act System of Records (SOR) notices prior to publication;
- Implementing Privacy Act and corresponding operating procedures; and
- Reviewing website privacy notices for accuracy.

3.1.6 HHS Office of Information Resources Management (OIRM), Information Collection Clearance Staff

The HHS OIRM is responsible for:

- Ensuring compliance with OMB directives on the Paperwork Reduction Act of 1995; and
- Providing guidance and assistance for compliance with the Paperwork Reduction Act.

3.2 OPDIV Level

Similar to the distribution of responsibilities at HQ, OPDIV CIOs are primarily responsible for overseeing the development and implementation of machine-readable privacy policies. As is the case for HQ activities, OPDIV CIOs may assign some responsibilities to OPDIV privacy contacts, Information System Security Officers (ISSOs), or other staff.

3.2.1 OPDIV Heads/Management Officials

OPDIV Heads/management officials are responsible for:

- Ensuring that roles with significant machine-readable privacy policy responsibilities are adequately staffed;

- Assuming responsibility for ensuring that machine-readable privacy policy responsibilities are assigned; and
- Working with CIOs to ensure that resources necessary for completing IT privacy and security tasks are allocated.

3.2.2 OPDIV CIOs

OPDIV CIOs are responsible for:

- Tracking and maintaining all machine-readable privacy policies;
- Reviewing completed machine-readable privacy policies and attesting that they are adequately and accurately completed;
- Ensuring that completed machine-readable privacy policies are implemented on all applicable OPDIV websites (existing and in development);
- Keeping management informed of machine-readable privacy policy resource needs; and
- Allocating proper resources to implement and maintain machine-readable privacy policies.

3.2.3 OPDIV ISSOs

OPDIV ISSOs are responsible for:

- Coordinating the completion and implementation of machine-readable privacy policies;
- Working with website owners to collect information needed to complete machine readable privacy policies; and
- Updating, at the direction of the OPDIV CIO/OPDIV management on the progress of machine-readable privacy policy completion, which enables the OPDIV CIO to monitor OPDIV wide progress and the effectiveness of the machine-readable privacy policy program.

3.2.4 Website Owners and Website Administrators

Website owners and website administrators are responsible for:

- Working with ISSOs, CIOs, or other staff to provide information relative to completing machine-readable privacy policies;
- Identifying any additional resources needed to complete machine-readable privacy policies;
- Implementing, testing, and maintaining machine-readable privacy policies on existing websites and websites in development; and
- Implementing, testing, and maintaining machine-readable policy reference files on any Web server that hosts an HHS website.

3.2.5 OPDIV Privacy Contact

Privacy contact duties include:

- Serving as a point of contact for issues related to the Privacy Act within the OPDIV;
- Serving as a resource for questions on acceptable website privacy practices; and
- Maintaining awareness of privacy laws, regulations, and issues.

A list of OPDIV privacy contacts is available at http://www.hhs.gov/contacts/privacy.html. Specific titles and job descriptions vary by OPDIV.

3.2.6 OPDIV Information Collection Clearance Officer

OPDIV Information Collection Clearance Officer is responsible for:

- Ensuring OPDIV compliance with OMB and Departmental directives on the Paperwork Reduction Act of 1995; and
- Providing guidance and assistance for compliance with the Paperwork Reduction Act.

3.2.7 Other Personnel

Staff completing machine-readable privacy policies may need to consult or coordinate with other OPDIV staff or subject matter experts. Specific job titles and job descriptions may vary by OPDIV. In general, however, such staff may include:

- IT specialists, Web masters, Web designers, and server administrators;
- Web content management staff, and other experts that will provide guidance and insight on enterprise-wide Web content configuration management practices. They may also provide guidance on mandatory website approval processes, agency design templates, website testing procedures, and Section 508 approval; and
- Other staff with responsibilities related to budgeting for IT, security, and privacy needs.

4.Machine-Readable Privacy Policy Process

According to federal requirements and guidance, HHS is responsible for developing and implementing machine-readable privacy policies on all public websites. To achieve compliance with this requirement, HHS should use the machine-readable privacy policy methodology detailed in this section.

4.1 Machine-Readable Privacy Policy Overview

This section provides a high-level summary of the methodology for implementing machine-readable privacy policies, including an explanation of the definition, purpose, objective, timing, and scope of machine-readable privacy policies. Reviewing this information will provide a better understanding of the context and framework for developing and implementing machine-readable privacy policies.

The machine-readable privacy policy methodology consists of preparing a questionnaire and creating, at a minimum, two extensible markup language (XML) files. The questionnaire is the Machine-Readable Data Analysis Worksheet, which efficiently collects all relevant data necessary to develop a machine-readable privacy policy.

As previously mentioned, two XML files will be created. The first file is the machine-readable privacy policy file. The machine-readable privacy policy file contains the information collected in the Machine-Readable Data Analysis Worksheet translated into XML. The second file is the machine-readable policy reference file. The machine-readable policy reference file maps the machine-readable privacy policy file to a website.

The methodology provides an effective framework for HHS to ensure website compliance with all relevant privacy laws, regulations, and guidance, including guidance generated from agencies external to HHS.

Refer to Appendix E for the Machine-Readable Data Analysis Worksheet.

4.2 Machine-Readable Privacy Policy Specification

In 2000, the W3C created a machine-readable privacy specification called P3P. The P3P specification includes a standard vocabulary for describing website data practices and a base data schema for describing the type of data collected.

Currently P3P is the only machine-readable privacy specification that complies with the requirements of Section 208 of the E-Government Act of 2002. Therefore, P3P has been chosen as the HHS standard for implementing machine-readable privacy policies. For the remainder of the document, the term machine-readable privacy policy and P3P can be used interchangeably.

4.3 Purpose of Machine-Readable Privacy Policy

Implementing machine-readable privacy policies will allow HHS to comply with Section 208 of the E-Government Act of 2002 by identifying and disclosing website privacy practices to the public. Specifically, machine-readable privacy policies will serve as a platform to:

- Ensure that website information collection and use practices conform to applicable legal, regulatory, and policy requirements;
- Examine and evaluate website data collection and data use practices to mitigate potential privacy risks; and
- Ensure that the public is accurately informed of website data collection and data use practices.

4.4 Benefits of a Machine-Readable Privacy Policy

Implementing machine-readable privacy policies supports E-Government goals of creating a citizen-centric government by increasing the effectiveness, efficiency, and quality of government services.

The benefits of a machine-readable privacy policy include:

- Compliance with Section 208 of the E-Government Act of 2002;
- Automatic access of a website's privacy practices;
- Increase in transparency of data collection and data use process, thus increasing the level of public trust in the Department;
- Increase in public confidence through anticipation of privacy concerns; and
- Improvement in awareness of potential privacy risks, exposures, and liabilities.

4.5 Timing

All HHS public websites should have an operational machine-readable privacy policy by June 15, 2005. Developing and implementing machine-readable privacy policies should occur at the beginning and throughout the development life cycle for HHS public websites. However, given the number of existing public websites owned by HHS, remediation of websites in the operation phase and mitigation of websites in the development phase must proceed simultaneously.

4.6 Scope

Machine-readable privacy policies should examine privacy practices that involve the collection, use, and disclosure of information on public websites. The machine-

readable privacy assessment requires that the website owners and developers answer privacy-related questions regarding the following:

- **Access:** Determine an individual's right to access their information collected by the website.
- **Data Categories:** Type of data collected.
- **Choices:** What choices users have on using their voluntary and mandatory collected data (opt-in vs. opt-out).
- **Usage:** For what business purpose data collected is used.
- **Sharing:** With whom data is shared, why, and whether sharing is optional.
- **Retention:** How long data collected is retained.
- **Dispute Resolution Mechanisms**: Legal rights or agency-created mechanisms that exist for the resolution of privacy-related disputes.
- **Expiration:** When the privacy policy expires.

5.Machine-Readable Privacy Policy Activities

This section provides the overarching steps in the machine-readable privacy policy activities from assigning responsibilities for completing machine-readable privacy policies to implementing the machine-readable privacy policy file on a Web server.

5.1 Step 1: Assign Roles and Responsibilities

Identify staff that will be responsible for creating and implementing machine-readable privacy policies on each website. Individuals may vary from a website owner (or IT lead) to an OPDIV's privacy contact. However, the OPDIV ISSO must accept responsibility for completing the machine-readable privacy policy implementation process or assign responsibility to a designated leader that possesses the knowledge and ability to understand all the possible issues, privacy-related, technical, and managerial that may arise during the creation and implementation of a machine-readable privacy policy.

5.2 Step 2: Create Website Inventory

Create an inventory of all websites. The website inventory should include website Uniform Resource Locator (URL), life cycle stage (maintenance or development), website Internet Protocol (IP) address, and website points of contact. The website inventory will be used to track and report progress on the machine-readable privacy policy implementation process.

5.3 Step 3: Assess Website Inventory for Public Websites

Based on the website inventory, determine which HHS websites (in development or maintenance) are defined as public websites. Only public websites are required to have a machine-readable privacy policy. Websites excluded from the machine-readable privacy policy requirement include:

- Information other than "government information" as defined in OMB Circular A-130;
- Agency intranet websites that are accessible only by authorized government users (employees, contractors, consultants, fellows, grantees); and
- Systems defined as national security systems under 40 U.S.C. 11103.

5.4 Step 4: Preparing the Machine-Readable Privacy Policy

Individuals assigned responsibility for developing and implementing machine-readable privacy policy should use the Machine-Readable Data Analysis Worksheet as the basis of the policy. Individuals should familiarize themselves with this document

prior to attempting to complete it. The Machine-Readable Data Analysis Worksheet is included in Appendix E of this document.

As users prepare to fill out the Worksheet, they will want to review the website's current human-readable privacy policy, gather information on website privacy practices from experts, and gain an understanding of how cookies are set and used on the website. Having a clear understanding of the website's information collection and use is critical to using the Worksheet and developing a machine-readable privacy policy.

While much of the information included in the machine-readable privacy policy may be included in the website's current human-readable privacy policy, the human-readable privacy policy may not be the only source of information for the machine-readable privacy policy. The machine-readable privacy policy is distinct in what information it requires and how it requires that information to be presented. While the human-readable privacy policy is a useful resource to the person developing a machine-readable privacy policy, it should not be the only source for assessing website privacy practices.

5.5 Step 5: Assess Website Privacy Practices

The most critical step for the success of implementing a machine-readable privacy policy is an understanding of a website's actual data practices. The goal of step 5 is to be able to answer the following questions:

- What is the website's URL and other website identifying information?
- What information is collected on the website?
- What is the purpose for collecting the information?
- How long is the information retained?
- Is the information shared?
- Is the information collection mandatory or voluntary?
- Does the website use cookies or third-party content?
- What federal privacy requirements apply to the website?
- When does the privacy policy expire?

Answering the above questions can be achieved by:

- Using this guide and the Machine-Readable Data Analysis Worksheet;
- Reviewing current human-readable privacy policy; and
- Interviewing website owners, business process experts, system administrators, Web developers, and privacy experts.

The information collected during step 5 should focus on the topics below and is the basic input for the Machine-Readable Data Analysis Worksheet and the final machine-readable privacy policy.

5.5.1 Website Identifying Information

Website identifying information refers to the technical and point of contact information that will be used in developing and implementing a machine-readable privacy policy. Table 1 illustrates all website identifying information that should be collected.

Table 1. Website Identifying Information

Website Identifying Information	Description/Purpose
Unique Project Identifier (UPI) Number	For E-Government Act tracking purposes; ensures project receives credit for fully implementing E-Government Act.
System of Records (SOR) Number	Identifies websites that are considered Privacy Act Systems.
Name of Organization	Name of organization responsible for the website.
Email address of individual responsible for website's privacy practices	The machine-readable privacy policy must include point of contact information for an individual that can claim responsibility for the website's privacy practices and the claims made in the website's privacy notices. This individual may be the OPDIV Privacy Contact or HHS' Privacy Act Officer.
Website URL implementing machine-readable privacy policy	The URL of the website that the machine-readable privacy policy is going to be on.
Website URL of human-readable privacy policy	The machine-readable privacy policy must include a reference to the website's human-readable privacy policy.
Hosting Web server name or IP address	The name or IP address of the Web server that hosts the website that is implementing a machine-readable privacy policy.
Website's primary point of contact (POC) information	The website's primary point of contact is the person responsible for oversight and management of the website. Information that should be collected includes name, email address, and telephone number.
POC information for website's technical support	Identifying the website's technical support team is important because they are resources during development and implementation of the machine-readable privacy policy. The technical support team should have an in-depth knowledge of website privacy practices. The technical support team will also be consulted during the implementation of the machine-readable privacy.
Website third-party content	Traditionally, third-party content refers to information contained on a website that is not maintained or created by the primary website content authors. The P3P specification expands the definition of third-party content to include images, frames, and other content served from a different Web domain than the page in which it is embedded.

Website Identifying Information	Description/Purpose
Third-party content source and machine-readable privacy policy status	If a website contains third-party content, the source of the third-party content and their machine-readable privacy policy status should be known and is useful for troubleshooting during the implementation and testing phases. If the website contains third-party content, all of the third-party content should have a machine-readable privacy policy for your website to be machine-readable privacy enabled. If the other website complies with your stated privacy policy, then the other website can create a policy reference file that refers to your machine-readable privacy policy file.
Machine-Readable Policy Name	Create a unique name for the website's machine-readable privacy policy. The policy name must be a single word without any spaces (e.g., website_policy, policy, cookie_policy). The policy name identifies which policy is being referenced. If your website has more than one machine-readable privacy policy, the policy name is used to identify which policy should be used.

5.5.2 Right to Access IIF

A right to access is the ability of an individual to view their IIF collected and stored on the website and address questions and concerns to the website. A right to access increases the transparency of information collection and provides an individual an opportunity to actively participate in the collection and storage process.

As a reminder, the E-Government Act of 2002 defines IIF as any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Some websites grant full access to view collected IIF, such as an e-commerce website that allows a person to view their name, address, and other IIF stored on the website. Other websites do not allow any access to IIF. Table 2 describes the six available categories in the P3P specification to describe access to data. Determining an individual's right to access is a requirement of the P3P specification.

Table 2. Right to Access IIF

Right to Access IIF	Description/Purpose
No Identified Data	Website does not collect identified data. Only websites that do not collect identified data may make this disclosure.
All Access	Website allows individuals to access all identified data. Only websites that provide access to all identified data that they collect may make this disclosure.
Identified Contact Information and Other Identified Information	Website allows individuals to access identified contact information and certain other identified information. These websites need not provide access to all such information.

Right to Access IIF	Description/Purpose
Identified Contact Information	Website allows individuals to access some or all identified contact information (e.g., name, address, and phone number).
Other Identified Information	Website allows individuals to access information other than identified contact information (e.g., subscription information, account information, preferences).
None	Website does not allow individuals to access any of their identified contact information.

5.5.3 Accountability

Accountability identifies dispute resolution mechanisms by which the website or HHS can be held accountable for complying with their stated privacy policies and federal guidelines. Dispute resolution mechanisms can be legal or HHS-created mechanisms that exist for the resolution of privacy-related disputes. Dispute resolution mechanisms can include any of the following:

- Customer service information, e.g., customer service representatives
- Independent verification organizations, e.g., Better Business Bureau
- Legal forum; e.g., court
- Applicable laws, e.g., the Privacy Act

HHS may also list the possible remedies to the dispute (e.g., money) in the case that a website fails to comply with their stated policies and federal guidelines.

Most, if not all, federal agency dispute resolution mechanisms will be categorized under the "applicable law" category with a possible dispute remedy as "law." All federal agencies are required by the E-Government Act to list the Privacy Act of 1974 as an applicable law. Many websites within HHS may also be required to list HIPAA and the COPPA. Table 3 lists the dispute resolution mechanisms available in the P3P specification. Determining the dispute resolution mechanism is a requirement of the P3P specification.

Table 3. Dispute Resolution Mechanisms

Dispute Resolution Mechanisms	Description/Purpose
Customer Service	Website should use this disclosure to indicate that they have customer service representatives that individuals can contact to attempt to resolve their disputes.
Independent Organization	Website should use this disclosure to describe an independent organization that individuals can contact to attempt to resolve their disputes.

Dispute Resolution Mechanisms	Description/Purpose
Court	Website should use this disclosure to indicate that individuals can file legal complaints against them to resolve disputes.
Applicable Law	Website should use this disclosure to indicate that disputes arising in connection with their privacy statements will be resolved in accordance to an applicable law.

5.5.4 Categories of Data Collected

Data collected on a website should be relevant and be the minimum amount of data necessary to complete the transaction. Data categories are a description of the type of data collected on a website. Table 4 describes the 17 available data categories in the P3P specification. The data collection categories must also indicate whether providing the data is optional. Optional is defined as whether the website requires visitors to submit the data. Optional data collection is also often referred to as voluntarily provided data. Section 208 of the E-Government Act requires that HHS inform visitors whenever providing requested information is voluntary or optional.

Table 4. Categories of Data Collected

Data Categories	Description/Purpose
Physical Contact Information	Information that allows an individual to be contacted in the "physical" world. Examples include postal address and phone number.
Online Contact Information	Information that allows an individual to be contacted on the Internet, examples include email address or personal website address.
Unique Identifiers	Non-financial pieces of information that are used to consistently identify or recognize an individual. Examples include a userID. Unique identifiers do not include government-identifies.
Purchase Information	Information actively generated by the purchase of a product or service, including information about the method of payment.
Financial Information	Information about an individual's finances. Examples include account balance, payment or overdraft history, and information about an individual's purchases or use of financial instruments, including credit or debit information.
Computer Information	Information about the computer system that an individual is using to access the network. Examples include IP address, domain name, browser type, and operating system. Does not include email addresses.

Data Categories	Description/Purpose
Navigation and Click Stream Data	Data generated by browsing a website. Examples include logs of what pages have been visited, how long visitors stayed on each page, and other information automatically logged by Web servers.
Interactive Data	Data actively generated from or reflecting explicit interaction with a service provider through its website. Examples include queries to search engines or account activity logs.
Demographic and Socioeconomic Data	Data actively generated from or reflecting explicit interaction with a service provider through its website. Examples include queries to search engines or account activity logs.
Content	The words and expressions contained in the body of a communication. Examples include email text, bulletin board postings or chat room text.
State Management Mechanism Data	Mechanisms for maintaining a user session or automatically recognizing users who have previously visited a particular website or accessed particular content. Cookies are the main mechanism for state management.
Political Information	Information about a membership in or affiliation with a civic or political organization. Examples include religious organizations, trade unions or professional associations.
Health Information	Information about an individual's physical or mental health and health-related topics. Examples include health care service or products, purchase of health care services or products or state of physical or mental health.
Preference Data	Information about an individual's likes and dislikes. Examples include musical tastes, favorite sports teams or answers to opinion questions.
Location Data	Information that can be used to identify a current physical location. Examples include Global Positioning System data.
Government Issued Identifiers	Information issued by the government for consistently identifying an individual. Examples include social security numbers or driver license numbers.
Other	Information that does not fall in any other category. A description of the information must appear in the human-readable privacy notice.

5.5.5 Purpose of Data Collection

Websites must disclose the reason data is being collected to ensure that the information being collected is narrow in scope and is used for specific purpose. Table 5 lists 12 purpose categories. More than one purpose can be chosen. The purpose categories can also indicate if the use of the information is based on consumer choice, by giving the purpose three attributes: always, opt-in, or opt-out. Always means that the user cannot opt-in or opt-out of the data usage and that the data

usage is always required. Opt-in data may be used for the purpose only when the user affirmatively requests the use. Examples include when a user checks a box to be added to a mailing list. Opt-out data may be used for the purpose designated, unless the user requests that it not be used in this way. Determining the purpose of the data collection is a requirement of the P3P specification. Designation of optional data is not a requirement; however it provides higher data collection transparency.

Table 5. Purpose of Data Collection

Purpose	Description/Purpose
Current	Completion and support of activity for which data was provided. Information may be used by the website to complete the activity for which it was provided. Occurrence of the activity may be once or multiple times.
Admin	Website and system administration information may be used for the technical support of the website and its computer system. Examples include log files that are used for maintaining the website, diagnosing server problems or detecting security breaches.
Develop	Research and Development information may be used to enhance, evaluate, or otherwise review the site, service, product, or market. This does not include personal information used to tailor content for a specific individual or information used to evaluate, target, profile, or contact an individual.
Tailoring	One-Time Tailoring information may be used to tailor or modify the content or design of the site for a single visit. Information must not be used for any kind of future customization beyond the current visit.
Pseudonymous Analysis	Information may be used to create or build a record of a particular individual or computer that is tied to a pseudonymous identifier without tying identified data (such as name, address, phone number or email address) to the record. The recorded profile will be used to determine the habits, interest or other characteristics of individuals for the purpose of research, analysis, and reporting, but it will not be used to attempt to identify specific individuals.
Pseudonymous Decision	Information may be used to create or build a record of a particular individual or computer that is tied to a pseudonymous identifier, without tying identified data (such as name, address, phone number, or email address) to the record. The recorded profile will be used to determine the habits, interest or other characteristics of individuals to make a decision that directly affects that individual, but it will not be used to attempt to identify specific individuals.

5.5.6 Data Recipients

Websites must disclose with whom they share information to ensure transparency and trust. Table 6 lists six available categories to describe data recipients. The data recipient categories may also indicate whether data sharing is required, an opt-in or an opt-out and a description of the entity. Disclosing data recipients is a requirement of the P3P specification. Indicating whether data sharing is required is optional.

Table 6. Data Recipients

Recipient	Description/Purpose
Ours	The data is used only by the entity referenced in the privacy policy, its agents, or parties for whom the entity is acting as an "agent." Agent is defined as a third party that processes data only on behalf of the entity for the completion of the stated purposes.
Delivery	The data may be used by entities performing delivery services and these delivery services may use the data for purposes other than completing the stated purpose. If the delivery services are contractually bound to use the data only for the stated purpose, then choose "ours" from above.
Same	The data is used by organizations that use data on their own behalf under equable practices. This recipient might be used to describe websites that share data with other agencies that have very similar privacy policies.
Other Recipient	The data is used by organizations that follow different privacy practices. The data may be used by organizations that are constrained by and accountable to the data collector, but may use the data in a way not specified in the data collector's privacy practices.
Unrelated	The data is shared with an organization whose data usage and practices are not known by the original data collector.
Public	The data may be published in public forums, such as bulletin boards, public directories, or commercial CD-ROM directories.

5.5.7 Data Retention Policies

Websites must inform visitors how long collected data is retained. Table 7 lists the five available data retention categories. The most commonly used categories will be "for the stated purpose," "as required by applicable law", or "no retention."

Table 7. Data Retention Policies

Data Retention	Description/Purpose
No Retention	Information is only retained for the time necessary to make use of it during a single online interaction. Information must be destroyed after the single interaction and cannot be kept or stored.

Stated Purpose	Information is retained briefly and destroyed at the earliest possible opportunity. The website human-readable privacy notice must have a data destruction timetable or a hyperlink to the data destruction timetable.
Legal Requirement	Information is kept to meet a stated purpose; however, the retention period is longer due to a legal requirement. The website human-readable privacy notice must have data destruction or a hyperlink to the data destruction timetable.
Business Practices	Information is retained for stated business purpose. The website human- readable privacy notice must have data destruction or a hyperlink to the data destruction timetable.
Indefinitely	Information is retained for an indefinite time.

5.5.8 Policy Expiration Date

Data expiration describes the lifetime of the machine-readable policy. The default expiration time is 24 hours. The default is generally determined to be an adequate expiry. If the default is not sufficient, websites can claim either a relative or absolute time of expiry. Table 8 lists the policy expirations.

Table 8. Policy Expiration

Expiration	Purpose
Default	The policy reference file and policy file have a life of 24 hours.
Absolute	The policy reference file and policy file have a lifetime expressed in Greenwich Mean Time (GMT). An example of GMT is Sun, 07 2008 08:49:37 GMT.
Relative	The policy reference file and policy file have a lifetime expressed in seconds from the time the response is sent from the original server. An example of a relative time of expiry is max-age "172800."

5.5.9 Conduct Cookie Analysis

Cookies are small bits of text that are sent to a website's HTTP headers. Cookies are stored on the computer and are used by websites to store identification numbers, information about your activities on the website, or information about the configuration options you have chosen on the website. Cookies come in two types: session and persistent. Session cookies expire at the end of a browser session. Persistent cookies remain on the computer over several browser sessions. Federal websites may only use session cookies, unless the website has obtained permission from the head of the agency.

With the advancement of customized browser settings, consumers have more control over how cookies are stored and accepted. The P3P specification has a policy option

to cover the use of cookies, called compact policies. The compact policies allow for website cookies, session or persistent, to be processed before a full machine-readable privacy policy is evaluated.

Creating a compact policy for cookies used on a website is optional; however, many Web browsers, such as Internet Explorer 6.0 and above, do not accept cookies that are considered "third-party" cookies that do not have a compact policy. For purposes of accepting cookies, the term third party refers to any content that originates from a different domain than the host.

If your website's functionality depends on setting third-party cookies or you are concerned with how first-party cookies are handled by the P3P specification and Web browsers, then the website should also include a compact policy.

A compact policy can be automatically generated by a machine-readable policy generator, such as the IBM P3P Editor, or the compact policy can be written manually in XML. Once completed, the compact policy is placed in the HTTP header. For more information on developing a compact policy, visit the W3C website http://www.w3.org/TR/P3P/#compact_policies.

5.6 Step 6: Complete the Machine-Readable Data Analysis Worksheet

The purpose of the Machine-Readable Data Analysis Worksheet is to serve as a tool to develop the basis of a machine-readable privacy policy. The Machine-Readable Data Analysis Worksheet is a series of questions based on the P3P specification and the information gathered during the website privacy practice assessment.
The Worksheet includes some pre-populated data. Pre-populated data indicates federally required information that must be included in all machine-readable privacy policy.

The completed Worksheet should reflect the website's actual data practices discovered during the website privacy practice assessment as well as all applicable privacy laws and regulations. For example, if your website must comply with the COPPA, you must include those privacy requirements in the machine-readable privacy policy.

The Machine-Readable Data Analysis Worksheet can be found in Appendix E.

5.7 Step 7: Determine Number of Machine-Readable Privacy Policies

The P3P specification enables websites to have an infinite number of machine-readable privacy policies. How many should be developed and implemented is a

decision each website owner must make after considering their website privacy practices and disclosure needs.

The simplest way to create a machine-readable privacy policy is to review the website's current human-readable privacy policy for accuracy and then translate the website's human-readable privacy policy into a single machine-readable privacy policy. This approach, while the easiest, is not the most accurate for agencies that must comply with a diverse set of federal privacy requirements, such as HIPAA, COPPA, or websites that must disclose the use of persistent cookies. Websites that have sections that handle data in different ways may want to create multiple machine-readable privacy policies with each machine-readable policy applying to a specific section of the website. Another option for websites that have multiple privacy requirements is to create a single machine-readable privacy policy that discloses all of the website's privacy practices.

For example, if an HHS website has a section that is geared toward children under the age of 13, the section of the website geared toward children must comply with COPPA website requirements. In this case, the individual developing the machine-readable privacy policy can either create two machine-readable privacy policies, one for each section of the website, or they can create one policy that encompasses all of the websites privacy practices, including COPPA.

In the above example, either approach is acceptable. The advantage of having multiple machine-readable privacy policies is that the individuals only receive privacy practices that apply to the website they are visiting, reducing user confusion or apprehension. The disadvantage is maintenance. Maintenance and administration of multiple machine-readable privacy policies is more challenging than maintaining one policy file.

5.8 Step 8: Select a Machine-Readable Privacy Policy Generator

The machine-readable privacy policy specification, P3P, is an XML standard. All machine-readable privacy policies and machine-readable policy reference files must be manually written in XML or generated using a machine-readable policy generator.

Machine-readable policy generators are tools that generate the machine-readable privacy policy and machine-readable policy reference file in XML without requiring the user to have knowledge of XML. In addition, most machine-readable privacy policy generators include a policy validation component to identify errors during the creation of the machine-readable privacy policy. Machine-readable policy generators are either Web-based, such as the P3PEdit tool, or downloadable, such as the IBM P3P Policy Editor. A complete listing of machine-readable policy generators can be found on the P3P Toolbox website (http://www.p3ptoolbox.org). The machine-readable privacy policy examples used in this document were created using IBM's P3P Policy Editor.

5.9 Step 9: Create the Machine-Readable Privacy Policy File

Creating a machine-readable privacy policy should be easy if correct information was gathered during the website privacy practice assessment and collected in the Machine-Readable Data Analysis Worksheet. Machine-readable policy generators are designed around a series of website privacy-related questions. Questions in the Machine-Readable Data Analysis Worksheet were designed for use with any machine-readable policy generator.

5.10 Step 10: Create a Machine-Readable Policy Reference File

A machine- readable policy reference file (PRF) is the method by which a user-agent, a P3P enabled web browser or software application, locates the machine-readable privacy policy that applies to the website so that the user-agent can process the machine-readable privacy policy file. In simpler terms, the PRF is a map that directs the user-agent to the appropriate policy file for the website. The PRF specifies the policy for a single Web page, sections of a website, or for an entire website. The PRF can refer to one or more policy files. This allows for one PRF to cover an entire website, even if different policy files apply to different pages of the website.

The PRF is created in XML and requires a specific syntax. Individuals implementing machine-readable privacy policies do not need to know XML to successfully create a PRF. Machine-readable privacy policy generators, such as the IBM P3P Editor, can generate PRFs.

Before creating a PRF, the following information should be known:

- Relative URL of the machine-readable privacy policy on the server;
- Which Web pages, sections of websites, or entire websites will be covered by the machine-readable privacy policy file;
- Web pages, sections of websites, or entire websites that are not covered by the machine-readable privacy policy;
- Web addresses of third-party content on other servers that are covered by the machine-readable privacy policy;
- Cookies that are or are not covered by the machine-readable policy file; and
- Machine-readable policy file expiration period.

PRFs can associate multiple machine-readable privacy policies to website URLs. In most cases, the PRF should only refer to content that is contained on the server that referenced the PRF. For example, if a machine-readable privacy policy is named hhsgov.p3p and it should apply to the website http://www.hhs.gov, then the PRF that associates hhsgov.p3p with http://www.hhs.gov must be on the same server as the HHS.Gov website. Exclusions to the rule are discussed in Step 11.

Associating Web content with a machine-readable privacy policy is flexible by using the PRF syntax. Using the PRF syntax, Web pages, images, directories within a Web server, or entire websites can be included or excluded from being associated with a machine-readable privacy policy. All INCLUDE and EXCLUDE URLs must be relative URLs. Table 9 gives examples of the PRF syntax.

Table 9. PRF Syntax Examples

PRF Syntax	Description/Purpose
<POLICY-REF about="#hhsgov"> <INCLUDE>/</INCLUDE> </POLICY-REF>	The machine-readable privacy policy "hhsgov" applies only to the home page of the chosen URL.
<POLICY-REF about="#hhsgov2"> <INCLUDE>/*</INCLUDE> </POLICY-REF>	The machine-readable privacy policy "hhsgov2" applies to the entire website, due to the use of the wildcard (*).
<POLICY-REF about="#hhsgov2"> <INCLUDE>/*</INCLUDE> <EXCLUDE>/</EXCLUDE> </POLICY-REF>	The machine-readable privacy policy "hhsgov2" applies to the entire website except the home page is excluded.
<POLICY-REF about="#hhsgov3"> <INCLUDE>/*.jpg</INCLUDE> <EXCLUDE>/*.pdf</EXCLUDE> </POLICY-REF>	The machine-readable privacy policy "hhsgov3" applies to all JPEGs and excludes PDFs on the website.

In some instances, PRFs can be combined with the machine-readable privacy policy. The advantage of combining the two files is that it reduces the number of Hyper Text Transfer Protocol (HTTP) requests to a website. Combining the policies can be used for agencies that only have a small number of Web servers. If an agency has a large number of Web servers, combining the two files may not be the best option due to the possible size of the file. For more information on writing a PRF, please visit the W3C website at http://www.w3.org/TR/P3P/#overview_of_prfs.

5.11 Step 11: Select Policy Reference File Locating Strategy

A PRF tells a user-agent, such as the IBM Privacy Bird or Internet Explorer 6.0 and above, the location of the machine-readable privacy policy locations; however, a method must also be used for the user-agent to find the PRF. Before saving the files to the Web server, a method for locating and retrieving the machine-readable policy file on the server must be determined.

The P3P specification includes three methods for locating a machine-readable privacy policy file. Each method has advantages and disadvantages; therefore, the individual responsible for implementation should consider local circumstances when choosing a method.

The machine-readable privacy policy file location methods include:

- Saving the policy file in the "well-known" location;
- HTTP requests; and
- Embedded LINK tags.

5.11.1 The Well-Known Location

The P3P specification has designated a file location for PRFs. The designated location is /w3c/p3p.xml and is informally called the "well-known" location. All user-agents automatically make the first HTTP GET request for the machine-readable privacy policy to the well-known location. The well-known location method takes precedence over any other location strategy.

Using the well-known location is the least complicated method because only one PRF needs to be created and administered and no other server or Web pages need to be specially configured. Using the well-known location may not be the best choice for websites that have a significant number (more than 100) machine-readable privacy policies. If a website has a significant number of machine-readable privacy policies, the size of the PRF will be large and will not transmit quickly.

The P3P specification considered different ports on a single host to be different websites. Therefore, if a website is specifying a port that should be used for information retrieval, then the website may need a separate policy reference file. This information is valuable when a website has both Secure Socket Layer and regular requests on the same server. For more information on the "well-known" location, please visit the W3C's Platform for Privacy Preferences 1.0 (P3P1.0) Specification (http://www.w3.org/TR/P3P/#overview_of_prfs).

5.11.2 HTTP Headers

The P3P specification defines a HTTP header that can be added to any HTTP request. A website might use the HTTP header method if the individual responsible for implementing and maintaining the PRFs does not have administrative access to use the well-known location on the Web server. The P3P HTTP header is:

P3P: policyref="URL"

If a website also includes a compact policy, then the P3P HTTP header uses the following syntax:

P3P: policyref="URL", CP="COMPACT POLICY TOKENS"

The following is a sample interaction between a client and server if the website uses the P3P HTTP header method instead of the well-known location:

Client request:

GET hhsprf.xml HTTP/1.1
Host:www.hhs.gov

Server response:

HTTP/1.1 200 OK
P3P: policyref=http://www.hhs.gov/hhsprf.xml
Content-Type: text/html

For specific information on configuring Web servers to add the P3P HTTP header, please visit the W3C's Platform for Privacy Preferences 1.0 (P3P1.0) Specification (http://www.w3.org/TR/P3P/#overview_of_prfs).

5.11.3 Embedded Link Tags

The third method for locating a PRF is an embedded HTML LINK tag. If the HTML LINK tag method is used, all HTML documents on a website must include the LINK tag in the HEAD of each HTML document. The following code demonstrates the LINK tag.

HEAD of HTML document:

<LINK rel="P3Pv1" href="URL of PRF">

LINK tag in HTML document (HHS.GOV):

```
<HTML>
<HEAD>
        <LINK rel="P3Pv1" href=http://www.hhs.gov/hhsprf.xml>
        <TITLE>Department of Health and Human Services</TITLE>
</HEAD>
<BODY>
<P> Welcome to the Department of Health and Human Services Home
Page.</P>
</BODY>
</HTML>
```

The HTML LINK tag method should be used if the person responsible for implementation and maintenance of the machine-readable privacy policies does not have access or administrative privileges over the Web server that contains the machine-readable privacy policy. The HTML LINK tag method does not associate non-

HTML content, such as images, Portable Document Formats or Word documents, with a machine-readable privacy policy. To associate non-HTML content with a machine-readable privacy policy, the content should be displayed after retrieving the HTML file.

For specific information on the HTML LINK tag method, please visit the W3C's Platform for Privacy Preferences 1.0 (P3P1.0) Specification (http://www.w3.org/TR/P3P/#syntax_link).

5.12 Step 12: Validate Machine-Readable Privacy Policies

Once implemented, machine-readable privacy policies must be validated to verify that the machine-readable privacy policies are accessible by P3P-enabled browsers and software. Validation of the machine-readable privacy policies should be conducted using a policy "validator." The W3C has a free policy validator available at http://www.w3.org/P3P/
validator.html. The W3C policy validator can verify integrated machine-readable policy files or independent policies.

5.13 Step 13: Maintaining Machine-Readable Privacy Policies

The requirement for having machine-readable privacy policies on public websites applies to websites that have been deployed as well as websites that are in the development process. To maintain compliance, a machine-readable privacy policy should be a requirement that is incorporated into Web design standards. Processes should be developed and documented for updating and maintaining the content and technical approach for the machine-readable privacy policy in the event of additional website privacy practice requirements.

In addition, websites should be continually monitored to verify that the machine-readable privacy policies are accessible and accurate. HHS is deploying a website monitoring capability, called Watchfire, which will assist in monitoring and maintaining machine-readable privacy policy compliance.

6.Conclusion

HHS must develop machine-readable privacy policies to satisfy the requirements of the E-Government Act and HHS Departmental policy. A well-thought-out machine-readable privacy policy, however, also presents HHS with the opportunity to determine whether it is complying with the requirements of the Privacy Act, COPPA, HIPAA and other federal legislation, regulations, and OMB memoranda. Furthermore, because the machine-readable privacy policies are publicly available, HHS is presented with an opportunity to assure the public that they are providing government services in a manner that is considerate of the sensitivity of the personal information they receive.

Appendix A: Document Feedback

This form is for reviewer-suggested corrections, revisions, or updates, and is intended to improve the usefulness of the document for possible inclusion in future versions. Please forward recommended changes and comments to the U.S. Department of Health and Human Services (HHS), Office of Information Resources Management (OIRM).

By E-mail: SecureOne.HHS@hhs.gov
Subject Line: Guidance Feedback
By Phone: (202) 690-6162

Document Title:
>
Section Number:
>

Category of Comment:	
A	Administrative. Administrative comments correct what appear to be inconsistencies between sections, typographical errors, or grammatical errors.
S	Substantive. Substantive comments are provided because sections in the publication appear to be or are potentially incorrect, incomplete, misleading, or confusing.
C	Critical. Critical comments will cause non-concurrence with the publication if concerns are not satisfactorily resolved.
M	Major. Major comments are significant concerns that may result in a nonoccurrence of the entire document if not satisfactorily resolved. This category may be used with a general statement of concern with a subject area, thrust of the document, etc., followed by detailed comments on specific entries in the publication which, taken together, constitute the concern.

Category	**Comment**

Name of Submitting Operating Division (OPDIV):
>
Your Name and Title:
>
Telephone:
>
E-mail:
>
Note: Use an additional blank sheet if needed.

Appendix B: Acronyms

CIO	Chief Information Officer
CSO	Chief Security Officer
COPPA	Children's Online Privacy Protection Act of 1998
FOIA	Freedom of Information Act
FR	Federal Register
FTC	Federal Trade Commission
GMT	Greenwich Mean Time
GPS	Global Positioning System
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
HQ	Headquarters
IIF	Information in Identifiable Form
ISSO	Information System Security Officer
IP	Internet Protocol
IT	Information Technology
M	Memorandum
NIST	National Institute of Standards and Technology
OCR	Office of Civil Rights
OIRM	Office of Information and Resources Management
OMB	Office of Management and Budget
OPDIV	Operating Division
PDF	Portable Document File
PHI	Protected Health Information
PIA	Privacy Impact Assessment
POC	Point of Contact
PRA	Paperwork Reduction Act
PRF	Policy Reference File
P3P	Platform for Privacy Preferences
SSL	Secure Socket Layer
SOR	System of Records
SP	Special Publication
W3C	World Wide Web Consortium
UPI	Unique Project Identifier
URL	Uniform Resource Locator
XML	Extensible Markup Language

Appendix C: Glossary

Compact Policy: A compact policy is an abbreviated version of the machine-readable privacy policy that describes the privacy practices associated with cookies.

eXtensible Markup Language (XML): A specification created by the World Wide Web Consortium. XML allows designers to create their own customized tags, enabling the definition, transmission, validation, and interpretation of data between applications and between organizations.

Cookie: Information that a website puts on an individual's computer so that it can remember something about the user at a later time. See also: persistent cookie, session cookie.

Human-Readable Privacy Policy: A human-readable privacy policy is a privacy policy written in a natural language (English). Every machine-readable privacy policy enabled website must have a human-readable privacy policy.

Information in Identifiable Form (IIF): Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. (Defined in *E-Government Act of 2002*, Pub.L.107-347, Section 208).

Intranet: A network based on TCP/IP protocols (an Internet) belonging to an organization, usually a corporation, accessible only by the organization's members, employees, or others with authorization.

Machine-Readable Policy File: An XML document that describes a website's privacy practices. Every machine-readable privacy policy-enabled website must have at least one machine-readable privacy policy.

Persistent Cookie: A cookie that is stored on the user's hard drive and remains there until the user deletes it or it expires.

Platform for Privacy Preferences (P3P): A specification created by the World Wide Web Consortium. P3P allows allow users' Web browsers to automatically understand websites' privacy practices.

Policy Reference File (PRF): A file using XML syntax that provides a map of where a website's machine-readable privacy policy (or policies) are located and which machine-readable privacy policy is associated with each directory, Web page, other Web resource, or cookie. It also provides information about how long the PRF is valid.

Session Cookie: A small file, stored in temporary memory, containing information about a user that disappears when the user's browser is closed. Unlike a persistent cookie, no file is stored on the user's hard drive.

Unique Project Identifier (UPI): An identifier that depicts agency code, bureau code, mission area (where appropriate), part of the exhibit where investment will be reported, type of investment, agency four-digit identifier, year the investment entered the budget, and mapping to the Federal Enterprise Architecture. For details and explanation, see OMB Circular A-11, Section 53.8.

User-agent: Web browsers or clients that are enabled to display and interpret machine-readable privacy policies.

Third-Party Content: The Platform for Privacy Preferences specification defines third-party content to include images, frames, and other content served from a different Web domain than the page in which it is embedded.

Third-Party Cookies: Internet Explorer 6.0 and above classifies any cookie that is being set from a domain other than the host as a third-party cookies. Third-party cookies that do not have compact policies are blocked by Internet Explorer 6.0 and above.

Website: A collection of interlinked Web pages (on either Internet or intranet sites) with a related topic, usually under a single domain name, which includes an intended starting file called a "home page." From the home page, access is gained to all the other pages on the website.

World Wide Web Consortium (W3C): A group of more than 500 companies, universities, and nonprofit organizations that work together to develop common protocols that promote the continued evolution and interoperability of the World Wide Web.

Appendix D: References

Cranor, Lorie. Web Privacy with P3P. Sebastopal, CA: O'Reilly & Associates, 2002.

Federal Trade Commission *Children's Online Privacy Protection Rule; Final Rule*, published in the Federal Register (FR) 64, 59887-59915, November 3, 1999.

Health and Human Services (HHS) Certification and Accreditation Guide, August 18, 2003.

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

OMB Circular A-130, *Management of Federal Information Resources,* Appendix III, *Security of Federal Automated Information Resources,* November 28, 2000.

OMB Memorandum (M), *Application of Subsection M of the Privacy Act,* November 30, 1979.

OMB M-99-18, *Privacy Policies on Federal Websites,* June 2, 1999.

OMB M-05-04, *Policies for Federal Agency Public Websites,* December 17, 2004.

OMB *Privacy Act Guidelines,* published in the Federal Register 40, 28934-28978, July 9, 1975.

OMB *Revised Supplemental Guidance for Conducting Computer Matching Programs,* FR 47, 21656-21658, May 19, 1982.

OMB *Supplementary Privacy Act Guidance,* FR 40, 56741-56743, December 4, 1975.

Public Law 93-579, *Privacy Act of 1974*, December 31, 1974.

Public Law 100-503, *Computer Matching and Privacy Act of 1988*, October 18, 1988.

Public Law 104-13, *The Paperwork Reduction Act of 1995*, May 22, 1995.

Public Law 104-191, *Health Insurance Portability and Accountability Act of 1996* (HIPAA), August 21, 1996.

Public Law 106-398, *Defense Authorization Act*, Title X, Subtitle G, *Government Information Security Reform Act* (GISRA), October 30, 2000.

Public Law 106-554, *Treasury and General Government Appropriations Act*, Section 515, *Guidelines for Ensuring and Maximizing the Quality Objectivity, Utility, and Integrity of Information Disseminated by Federal Organizations,* February 22, 2002.

Public Law 107-347 [H.R. 2458], *The E-Government Act of 2002*. Title III of this Act is the *Federal Information Security Management Act of 2002* (FISMA), December 17, 2002.

US Code, 12 U.S.C. 3401 et seq., *Right to Financial Privacy Act of 1978.*

US Code, 15 U.SC. § 6501 et seq., *Children's Online Privacy Protection Act of 1998*.

Appendix E: Machine-Readable Data Analysis Worksheet

Section 208 of the E-Government Act requires that all public federal websites implement a machine-readable privacy policy. The Platform for Privacy Preferences (P3P) has been selected as the standard machine-readable privacy policy standard. The Machine-Readable Data Analysis is the basis for determining a public website's data practices as they pertain to Section 208 and P3P. The Machine-Readable Data Analysis will assess an agency's public website data practices for the following:

- **Access**—If individuals can access their information collected by the website
- **Dispute Resolution Mechanisms**—Legal rights or agency-created mechanisms that exist for the resolution of privacy-related disputes
- **Data Categories**—Type of data collected
- **Purpose**—For what business purpose data collected is used
- **Recipients**—With whom data is shared, why, and whether sharing is optional
- **Retention**—How long data collected is retained
- **Expiration**—When the privacy policy expires

Questions marked with an asterisk (*****) indicates that an answer is required as part of the P3P data schema or by federal privacy legislation or guidelines. The questions contained in the worksheet have been chosen for their relevancy to implementing a machine-readable privacy policy. It is suggested that an accurate answer be provided for all questions included in the worksheet.

The Worksheet includes some pre-populated data. Pre-populated data indicates federally required information that must be included in all machine-readable privacy policy.

For questions related to the technicalities of privacy laws, please contact the HHS Privacy Act Officer or HHS Privacy Advocate.

Website Identifying Information	
Unique Project Identifier Number:	
System of Records Number:	
Name of Organization*****:	
Email address of individual responsible for website's privacy practices*****:	
Phone Number for Privacy Complaints:	
Postal Address for Receiving Written Privacy Complaints:	
Website URL implementing machine-readable privacy policy*****:	http://
Website URL of Current Human-Readable Privacy Notice*****:	http://

Website Technical/Contact Information			
	Hosting Web Server Name or IP Address:		
	Name of the website's Primary Point of Contact (POC):		
	Website Primary POC Phone Number:		
	Website Primary POC Email Address:		
	Name of website's Technical Support (Web master or system administrator):		
	Technical Support Phone Numbers:		
	Technical Support Email Addresses:		
	Does the website Contain Persistent Tracking Technology (persistent cookies, Web bugs, Web beacons)*:	☐ Yes	No
	Does the website Contain Third-Party Content (See Appendix C for definition of third-party content) *:	☐ Yes	No
	If yes, What is the Third-Party Contents Source*:	http://www.123.1234	
	Does the Third-Party Content Have a Machine-Readable Privacy Policy*:	☐ Yes	No
	Machine-Readable Policy Name**—** Name your machine-readable privacy policy. The policy name must be a single word without any spaces (e.g., *website_policy*, *policy*, *cookie_policy*). The policy name identifies which policy	Policy Name:	

	is being referenced. If your website has more than one machine-readable privacy policy, the policy name is used to identify which policy should be used.	

No.	Machine-Readable Question Sets	User Responses
Access*: Access is the ability of an individual to view his or her information in identifiable form (IIF) and address questions or concerns to the website. Access is a mandatory element. There are six available access categories. Choose the access category that applies to the type of data collected on the website. For a definition of data categorized as IIF, please go to Appendix C, Glossary.		
1	☐ **No Identified Data—** Website does not collect IIF. Only websites that do not collect IIF may make this disclosure.	
	☐ **All Access—**Website allows individuals to access all IIF. Only websites that provide access to all IIF that they collect may make this disclosure.	
	☐ **Identified Contact Information & Other Identified Information—** Website allows individuals to access their contact information and other IIF. These websites need not provide access to all such information.	
	☐ **Identified Contact Information—** Website allows individuals to access some or all of an individual's contact information (e.g., name, address, phone number).	
	☐ **Other Identified Information—** Website allows individuals to access information other than an individual's contact information (e.g., subscription information, account information, preferences).	
	☐ **None—**Website does not allow individuals to access any of their IIF.	

No.	Machine-Readable Question Sets	User Responses
Dispute Resolution Mechanisms*: Dispute resolution data identifies legal or agency-created mechanisms that exist for the resolution of privacy-related disputes. Dispute resolution mechanisms can include customer service information, independent verification organizations (such as the Better Business Bureau), and legal forums or applicable laws (such as the Privacy Act). The agency may also list the possible remedies in case a website fails to comply with applicable privacy legislation and privacy notices. Most, if not all, federal agency dispute resolution mechanisms will be categorized under the "applicable law" category with a possible dispute remedy as "law." All federal agencies are required by the E-Government Act to list the *Privacy Act of 1974* as an "applicable law."		
2	☐ **Customer Service—** Website should use this disclosure to indicate that they have customer service representatives that individuals can contact to attempt to resolve their disputes.	Customer Service Contact Information (required): Customer Service URL (required): Logo URL (optional): Remedies (optional): ☐ Correct ☐ Money ☐ Law Description (required):
	☐ **Independent Organization—** Website should use this disclosure to describe an independent organization that individuals can contact to attempt to resolve their disputes.	Organization Name (required): Organization URL (required): Logo URL (optional): Remedies (optional): ☐ Correct ☐ Money ☐ Law Description (required):
	☐ **Court—**Website should use this disclosure to indicate that individuals can file legal complaints against them to resolve disputes.	Name of Legal Forum (required): Legal Forum URL (required): Logo URL (optional): Remedies (optional): ☐ Correct ☐ Money ☐ Law Description (optional):
	☒ **Applicable Law*—**Website should use this disclosure to indicate that disputes arising in connection with their privacy statements will be resolved in accordance to an applicable law.	Name of Law (required): The Privacy Act of 1974 Applicable Law URL (required): http://www.usdoj.gov/foia/privstat.htm Logo URL (optional): Remedies (optional): ☐ Correct ☐ Money ☐ Law Description (optional):

No.	Machine-Readable Question Sets	User Response
Data Categories*: Data categories are a description of the type of data collected on a website. There are 17 available data categories. Choose the data category that applies to the type of data collected on the website. More than one category may be chosen. The data collection categories must also indicate if the collection of the information is optional. Optional is defined as whether the website requires visitors to submit the data. Optional data collection is also often referred to as voluntarily provided data. Section 208 of the E-Government Act requires that agencies inform visitors whenever providing requested information is voluntary.		
3	☐ **Physical Contact Information**— Information that allows an individual to be contacted in the "physical" world. Examples include postal address and phone number.	**Input*:** ☐ Optional/Voluntary
	☐ **Online Contact Information**— Information that allows an individual to be contacted on the Internet. Examples include email address or personal website address.	**Input*:** ☐ Optional/Voluntary
	☐ **Unique Identifiers**—Non-financial pieces of information that are used to consistently identify or recognize an individual. Examples include a userID. Unique identifiers do not include government-identifies.	**Input*:** ☐ Optional/Voluntary
	☐ **Purchase Information**— Information actively generated by the purchase of a product or service, including information about the method of payment.	**Input*:** ☐ Optional/Voluntary
	☐ **Financial Information**— Information about an individual's finances. Examples include account balance, payment or overdraft history, and information about an individual's purchase or use of financial instruments, including credit or debit information.	**Input*:** ☐ Optional/Voluntary

	☐ **Computer Information**—Information about the computer system that an individual is using to access the network. Examples include IP address, domain name, browser type, and operating system. Does not include email addresses.	**Input*:** Optional/Voluntary
	☐ **Navigation & Click Stream Data**—Data generated by browsing a website. Examples include logs of what pages have been visited, how long visitors stayed on each page, and other information automatically logged by Web servers.	**Input*:** Optional/Voluntary
	☐ **Interactive Data**—Data actively generated from or reflecting explicit interaction with a service provider through its website. Examples include queries to search engines or account activity logs.	**Input*:** Optional/Voluntary
	☐ **Demographic & Socioeconomic Data**—Data actively generated from or reflecting explicit interaction with a service provider through its website. Examples include queries to search engines or account activity logs.	**Input*:** Optional/Voluntary
	☐ **Content—**The words and expressions contained in the body of a communication. Examples include email text, bulletin board postings, or chat room text.	**Input*:** Optional/Voluntary
	☐ **State Management Mechanism Data**—Mechanisms for maintaining a stateful session with a user or automatically recognizing users who have previously visited a particular website or accessed particular content. Cookies are the main mechanism for state management.	**Input*:** Optional/Voluntary

	☐ **Political Information—** Information about a membership in or affiliation with a civic or political organization. Examples include religious organizations, trade unions or professional associations.	**Input*:** Optional/Voluntary
	☐ **Health Information—** Information about an individual's physical or mental health and health-related topics. Examples include health care service or products, purchase of health care services or products or state of physical or mental health.	**Input*:** Optional/Voluntary
	☐ **Preference Data—** Information about an individual's likes and dislikes. Examples include musical tastes, favorite sports teams, or answers to opinion questions.	**Input*:** Optional/Voluntary
	☐ **Location Data—** Information that can be used to identify a current physical location. An example is GPS data.	**Input*:** Optional/Voluntary
	☐ **Government Issued Identifiers—** Information issued by the government for consistently identifying an individual. Examples include social security numbers or driver license numbers.	**Input*:** Optional/Voluntary
	☐ **Other—**Information that does not fall in any other category. A description of the information must appear in the human-readable privacy notice.	**Input*:** Optional/Voluntary **Description***:

No.	Machine-Readable Question Sets	User Response
Purpose*: Describes the purpose for which data is collected. Websites must disclose all that apply to their data practices. There are 6 purpose categories to choose from. More than one purpose can be chosen. The purpose categories can also indicate if the use of the information is based on consumer choice, by giving the data usage three attributes: (1) always, (2) opt-in or (3) opt-out. Always means that the user cannot opt-in or opt-out of the data usage and that the data usage is always required. Opt-in data may be used for the purpose only when the user affirmatively requests the use. Examples include when a user checks a box to be added to a mailing list. Opt-out data may be used for this purpose unless the user requests that it not be used in this way. Designation of optional data is not a requirement; however, it provides higher data collection transparency to the consumer.		
4	☐ **Current**—Completion and support of activity for which data was provided. Information may be used by the website to complete the activity for which it was provided. Occurrence of the activity may be once or multiple times.	
	☐ **Admin**—Website and system administration information may be used for the technical support of the website and its computer system. Examples include log files that are used for maintaining the website, diagnosing server problems, or detecting security breaches.	**Input** (optional)**:** ☐ Always ☐ Opt-In ☐ Opt-Out
	☐ **Develop**—Research and Development information may be used to enhance, evaluate, or otherwise review the site, service, product, or market. This does not include personal information used to tailor content for a specific individual or information used to evaluate, target, profile, or contact an individual.	**Input** (optional)**:** ☐ Always ☐ Opt-In ☐ Opt-Out
	☐ **Tailoring**—One-Time Tailoring information may be used to tailor or modify the content or design of the site for a single visit. Information must not be used for any kind of future customization beyond the current visit.	**Input** (optional)**:** ☐ Always ☐ Opt-In ☐ Opt-Out

	☐ **Pseudonymous Analysis**—Information may be used to create or build a record of a particular individual or computer that is tied to a pseudonymous identifier, without tying identified data (such as name, address, phone number, or email address) to the record. The recorded profile will be used to determine the habits, interest or other characteristics of individuals *for the purpose of research, analysis, and reporting*, but it will not be used to attempt to identify specific individuals.	**Input** (optional)**:** In Opt-Out	Always	Opt-
	☐ **Pseudonymous Decision**—Information may be used to create or build a record of a particular individual or computer that is tied to a pseudonymous identifier without tying identified data (such as name, address, phone number or email address) to the record. The recorded profile will be used to determine the habits, interest or other characteristics of individuals *to make a decision that directly affects that individual,* but it will not be used to attempt to identify specific individuals.	**Input** (optional)**:** In Opt-Out	Always	Opt-

No.	Machine-Readable Question Sets	User Response
Recipients*: Recipients describes with whom collected data is shared. Websites must disclose with whom they share data. There are six available recipient categories. More than one category may be chosen. The data recipient categories may also indicate whether or not data sharing is required, an opt-in or an opt-out and a description of the entity. Please note, information that may be shared for law-enforcement purposes is included in the "ours" recipient disclosure and does not require a special disclosure.		
5	☐ **Ours—**The data is used only by the entity referenced in the privacy policy, its agents, or parties for whom the entity is acting as an "agent." Agent is defined as a third party that processes data only on behalf of the entity for the completion of the stated purposes.	**Description** (optional):
	☐ **Delivery—**The data may be used by entities performing delivery services and these delivery services may use the data for purposes other than completing the stated purpose. If the delivery services are contractually bound to use the data only for the stated purpose, then choose "ours" from above.	**Recipient Required** (optional)**:** ☐ Always ☐ Opt-In ☐ Opt-Out **Description** (optional):
	☐ **Same—**The data is used by organizations that use data on their own behalf under equable practices. This recipient might be used to describe websites that share data with other agencies that have very similar privacy policies.	**Recipient Required** (optional)**:** ☐ Always ☐ Opt-In ☐ Opt-Out **Description** (optional):
	☐ **Other Recipient—**The data is used by organizations that follow different privacy practices. The data may be used by organizations that are constrained by and accountable to the data collector, but may use the data in a way not specified in the data collector's privacy practices.	**Recipient Required** (optional)**:** ☐ Always ☐ Opt-In ☐ Opt-Out **Description** (optional):

	☐ **Unrelated—**The data is shared with an organization whose data usage and practices are not known by the original data collector.	**Recipient Required** (optional)**:** Always Opt-In Opt-Out **Description** (optional):
	☐ **Public—**The data may be published in public forums, such as bulletin boards, public directories, or commercial CD-ROM directories.	**Recipient Required** (optional)**:** Always Opt-In Opt-Out **Description** (optional):

No.	Machine-Readable Question Sets
Retention*: For all data elements collected, indicate the data-retention policy. Indication of a data-retention policy is required. Most federal agencies will indicate "for the stated purpose," "as required by applicable law," or "no retention" under the data retention categories.	
6	☐ **No Retention—**Information is only retained for the time necessary to make use of it during a single online interaction. Information must be destroyed after the single interaction and cannot be kept or stored.
	☐ **Stated Purpose—**Information is retained briefly and destroyed at earliest possible opportunity. The website human-readable privacy notice must have a data destruction or a hyperlink to the data destruction timetable.
	☐ **Legal Requirement—**Information is kept to meet a stated purpose; however the retention period is longer due to a legal requirement. The website human-readable privacy notice must have data destruction or a hyperlink to the data destruction timetable.
	☐ **Business Practices**—Information is retained for stated business purpose. The website human-readable privacy notice must have data destruction or a hyperlink to the data destruction timetable.
	☐ **Indefinitely**—Information is retained for an indefinite time.

No.	Machine-Readable Question Sets	User Response
Data Expiration*: Data expiration describes the lifetime of the policy or policy reference file. Policy expiration is used to determine when a user-agent must request a website's policy file or policy reference file. The default expiry time is 24 hours. The default is generally determined to be an adequate expiry. If the default is not sufficient, websites can claim either a relative or absolute time of expiry.		
7	☐ **Default**—The policy reference file and policy file have a life of 24 hours.	
	☐ **Absolute—**The policy reference file and policy file have a lifetime expressed in Greenwich Mean Time (GMT). An example of GMT is Sun, 07 2008 08:49:37 GMT.	GMT:
	☐ **Relative—**The policy reference file and policy file have a lifetime expressed in seconds from the time the response is sent from the original server. An example of a relative time of expiry is max-age "172800."	Max-Age:

Appendix F: Information Security Program Documents

The Department of Health and Human Service (HHS) Information Technology Security Program is supplemented by a series of HHS Information Security documents. These documents include:

- HHS Information Security Program Policy
- HHS Information Security Program Handbook
- HHS Information Security Program Rules of Behavior
- Baseline Security Requirements Guide
- Certification and Accreditation (C&A) Guide
- Configuration Management Guide
- Contingency Planning for Information Security Systems Guide
- Critical Infrastructure Protection (CIP) Planning Guide
- Data Cryptography Guide
- Disaster Recovery Planning Guide
- Firewall Configuration Guide
- Health Insurance Portability and Accountability Act (HIPAA) Compliance Guide
- Incident Response Planning Guide
- Information Privacy Program Policy
- Information Privacy Program Handbook
- Information Technology (IT) Penetration Testing Guide
- IT Personnel Security Guide
- IT Physical and Environmental Security Guide
- IT Privacy Impact Assessment Guide
- IT Security Capital Planning Guide
- Machine-Readable Privacy Policy Guide
- Plan of Actions and Milestones (POA&M) Guide
- Risk Assessment Guide
- Security Test and Evaluation (ST&E) Planning Guide
- Web Security Guide
- Wireless Security Program Development Guide

Acknowledgements

Deanna Dicarlantonio and Marcela Souaya were instrumental in the development of this document.