SAMHSA WEB POLICY

Part 2: DMS-IT Technical Guidelines

June 2006

Contents

SAMHSA, an agency within the U.S. Department of Health and Human Services, is the lead Federal agency
For improving the quality and availability of substance abuse prevention, addiction treatment,
and mental health services in the United States.

Part 2: SAMHSA Web Standards
DMS-IT Technical Guidelines for GPOs and Web site Contractor Technical Staff

Last Revised April 2006

Approval and Update Procedures

Pre-Development Meeting

A meeting with the SAMHSA Webmaster, the Office of Communications (OC), the Government Project Officer (GPO) and Technical Contractor Staff must be held prior to any Web site development. This meeting is held for a general debriefing of the Web site concept, development and implementation procedures and expected deliverable standards to be followed. The SAMHSA Web Guidelines and the SAMHSA Checklist for New/Migrated Web sites are provided to the GPO and their Technical Contractor Staff at this meeting. Once the Checklist has been completely filled out, it must be submitted to **Webmaster@samhsa.hhs.gov**. The official HHS/SAMHSA Clearance Form 524A must be submitted and approved by OC before any Web site development begins.

Any technical specifications of the Web site setup and design (including software packages to be used, programming languages to be used, client requirements, etc.) must be submitted to the SAMHSA Webmaster at this time.

In addition, functional requirements need to be discussed to determine if specific policies, procedures and regulations need to be followed.

NOTE: Any changes to the functional requirements discussed in this meeting, prior to deployment, must be communicated to the SAMHSA Webmaster. An e-mail detailing the changes (i.e., new forms, new databases, personal information collection, product sales, new coding styles,) needs to be sent to **Webmaster@samhsa.hhs.gov**.

Web Site Hosting

Web sites developed for SAMHSA are required to be housed on SAMHSA's servers, once development has been completed. Exceptions to this rule may be given, based on a projects scope and other factors, by the SAMHSA Webmaster.

Web Site Approval Process

Web site design and layout (including the site map) must be approved by SAMHSA once a prototype of the Web site has been completed. This prototype is typically placed on a SAMHSA Beta Server or on the Contractor's Development Server if hosted offsite.

In order to request a prototype approval, the Contractor will send an e-mail to the Government Project Officer (GPO) and the SAMHSA Webmaster making them aware that the prototype is ready for review.

Once the Web site development has been completed, the GPO must request a formal and final review of the Web site. This review is conducted by SAMHSA's OC before the official launch.

FILE FORMATS for HTML CONVERSION: When submitting source files to SAMHSA DMS-IT staff for conversion to HTML, files in Microsoft Office formats (Word, Excel, PowerPoint, etc.) are strongly preferred. Other formats may be considered on a case-by-case basis, but may not be acceptable due to level of effort required for conversion.

Web Site Post/Update Procedures—SAMHSA Hosted Sites

New content must be submitted to the Webmaster via e-mail for posting to SAMHSA's Beta Server for review by the Government Project Officer (GPO). Any content which falls under the categories listed in "Concept and Content Clearance" in Part 1: Web Content Guidelines on Page 3 of this Policy will require OC approval before being posted live. Once the GPO and OC have approved the new content, the SAMHSA Web Team will migrate the changes to the live Web site. All e-mails to Webmaster must include:

- A zip file containing only the files that need to be posted to the site,
    - Files appropriately small in number and/or in size do not need to be zipped
- A description of the content or database being added to the site,
- A cc: sent to the GPO, and
- A cc: sent to the OC via **rich.morey@samhsa.hhs.gov**.

Updated content must be submitted to the Webmaster via e-mail for posting to SAMHSA's Beta Server for review by SAMHSA GPO. Once the GPO has approved the updates, the SAMHSA Web Team will migrate the changes to the live Web site. All e-mails to Webmaster must include:

- A zip file containing only the files that need to be posted to the site,
- A description of the content or database code updates being made, and
- A cc: sent to the GPO.

All communications, including update procedures, are conducted with SAMHSA support staff via the "**Webmaster@samhsa.hhs.gov**" e-mail account.

All proposed postings (whether new or updates) must be submitted by the GPO (not the Contractor) to the SAMHSA Webmaster; otherwise they will not be posted.

Post and Update Procedures for Third Party Hosted Sites

New content* must be posted to the Contractor's Development Server for review and approval by the GPO BEFORE posting to the live public site. Any content listed under "Concept and Content Clearance" in Page 3 of this Policy requires OC clearance prior to public release, and DMS-IT staff will not post it until clearance is granted. Once the GPO has approved the updates via written communication, the Contractor may migrate the changes to the live Web site.

Contractors must send all communications regarding updates via e-mail to the GPO and include:

- A description of the content or database code updates being made,
- The URL where the beta site can be viewed,
- A cc: sent to the SAMHSA Webmaster at **Webmaster@samhsa.hhs.gov**, and
- A cc: sent to the OC via **rich.morey@samhsa.hhs.gov** for content clearance (if required).

Updated content which does not require OC clearance must be posted to the Contractor's Development Server for review and approval by the GPO BEFORE posting to the live public site. Once the GPO has approved the updates via written communication, the Contractor may migrate the changes to the live Web site.

*** NOTE:** New content is defined as stated in this Policy under Part I, Concept and Content Clearance, plus any additional Web pages (files) that have been added to the site and were not previously present on that site**.**

Infrastructure Standards

Hardware Requirements

Any unique or specific hardware requirements beyond the norm for a Web site (e.g., proprietary hardware, large volumes of hard drive space, extra server(s)), require the prior approval from DMS-IT.

Software Requirements

The following is a list of software that SAMHSA currently supports for Web site development. Prior approval from DMS-IT is required if software, other than what is listed below, is to be used for Web site development.

- **Web Server Operating Systems**: Windows 2000, IIS 5+
- **Database Technologies**: SQL Server 2000, Oracle 8+
- **Browser Technologies**: MS Internet Explorer (IE) 6+, Netscape Navigator 7+
- **Server Technologies**: ASP, ASP.NET, Oracle 9i Application Server, Cold Fusion 7 – (For existing systems only)

Prohibited/Restricted Web Technologies

Unless prior written approval is obtained from the SAMHSA Webmaster, Web site and applications developed by SAMHSA contractors (on or offsite) are prohibited from using the following:

- Lotus Notes "Domino" Web sites
- Cold Fusion Web sites (Require Special Approval from DMS-IT. Existing Cold Fusion systems are “grandfathered” until such time as they can be migrated to a new platform at minimal cost and interruption.)
- Microsoft FrontPage Extensions
- ‘Forums' or ‘Bulletin Board' areas on public SAMHSA Web sites (pages where users can directly upload content to SAMHSA Web pages; if allowed, content posted must be held pending approval by a content expert)
- Real-time Web chat and Instant Messenger
- List Servs
- RealAudio/Video

These restrictions apply to any technology that cannot be implemented using the software indicated in above.

New Web Technologies are constantly emerging. It is not DMS-IT's intent to be restrictive about these technologies. Rather, the intent is to provide sensible solutions to the needs of each site. By the same token, SAMHSA cannot possibly offer or support every Web application or component on the market. If DMS-IT does not currently offer a technology you would like to use, a decision may be made to do so based on joint needs, capabilities, and other factors. It is essential, however, that the Government Project Officer (GPO) ensures that the Web sites meet DMS-IT requirements before development work begins.

SAMHSA Beta Server Access

SAMHSA’s Beta Servers are for internal staff use only, and can only be accessed from the SAMHSA Network, which is inside the SAMHSA firewall. If Contractors wish to view their site on SAMHSA’s Beta Server, they must come into the SAMHSA building to do so.

External contractors, with the exception of the DMS-IT contract staff, are not authorized to perform work on any server hosted at SAMHSA.   On occasion, HTTP access may be granted to external Contractors for the purposes of viewing the Beta Site using a Web Browser. Such access is rare. Permission must be obtained via the SAMHSA Webmaster.

Administration Tools

IIS Web-based Administration tools are disabled on SAMHSA public Web servers. Management is accomplished by the Webmaster or designated through the Microsoft Management Console (MMC).

In addition, the Cold Fusion (CF) Administrator will not be installed on any virtual sites that are available to the Public. CF Administrator is available on its own virtual site which has been firewall restricted to only SAMHSA staff.

Web Site Development Standards

General Web Site Development Standards

Unless decided otherwise by the SAMHSA Webmaster (with input from the OC), new sites will be posted as a new virtual Web, facilitating:

- ease of management/reporting,
- limited ‘bloating’ under www directories, and
- separation of processes for monitoring and troubleshooting.

New Virtual Webs are hosted using an IP address versus Host Headers, unless decided otherwise by the SAMHSA Webmaster. No duplication of files is allowed. Links must be used instead.

Browser Requirements

All Web sites must be designed for 800x600 screen resolution and must function properly in both Netscape Navigator 7 (or greater) and MS Internet Explorer 6 (or greater).

Web Site Cookies

SAMHSA follows the HHS IRM Policy for Usage of Persistent Cookies (HHS-IRM-2000-0009). This policy is available at **www.hhs.gov/read/irmpolicy/index.html** and states:

"Persistent" Web cookies shall not be used on HHS Web sites, or by contractors when operating Web sites on behalf of HHS agencies, unless the following conditions are met:

- The site gives clear and conspicuous notice;
- There is a compelling need to gather the data on the site;
- Appropriate and publicly disclosed privacy safeguards exist for handling any information derived from the cookies; and
- The HHS Secretary gives personal prior approval for the use.

"Persistent" Web cookies are defined as Web cookies that can track "the activities of users over time and across different Web sites."

"**Session" Web cookies** do not fall within the scope of this policy. Exempted cookies include those that retain information only during the session or for the purpose of completing a particular online transaction, without any capacity to track users over time and across different Web sites. (Examples: for using shopping carts to purchase a number of items online or for filling out applications that require accessing multiple Web pages.)

508 Compliancy

All government funded Web sites must comply with the requirements of Section 508 of the Rehabilitation Act (29 U.S.C. 794d). Section 508 requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), Federal employees with disabilities have comparable access to and use of information and data as Federal employees who have no disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have comparable access to and use of information and data as the public without disabilities, unless an undue burden would be imposed on the agency. For more detailed information, go to **http://www.Section508.gov**.

508-compliance is the responsibility of each Web site's development staff. The official software used by HHS and SAMHSA to check for 508 compliance is WatchFire WebXM. (This is provided for information purposes only. Contractors are neither required nor expected to purchase the WebXM product).

In general, the following must be adhered to:

- All sites developed must function properly in both Netscape Navigator 7 (or greater) and MS Internet Explorer 6 (or greater).
- If third-party browser plug-ins for Netscape or Internet Explorer are needed, prior testing and approval of the plug-ins by DMS-IT is required. Requests should be sent to the SAMHSA Webmaster at **Webmaster@samhsa.hhs.gov.**
- Linking to external Web sites, which do not comply with Section 508 Accessibility regulations, is allowed provided that an Exit Disclaimer is used. (See Exit Disclaimer Section of this document for exit disclaimer language).
- If a PDF file is used on a Web site, a text equivalent must also be provided. (A Section 508 accessible HTML version qualifies as a text equivalent version.) If this is not possible, users who require it must be given another way to get the information they seek (such as ability to order and receive a printed copy).
- Reminder: All graphic files that directly relate to the context of a document must have a text equivalent available. This includes graphics which reside in MS PowerPoint slides.

208 Compliancy

All Web sites developed must comply with the E-Government Act of 2002, Section 208. As of June 2005, SAMHSA translated all of their Human-Readable Privacy Policies into a standardized Machine-Readable format. During this process, SAMHSA was able to identify 1 master human-readable privacy policy (P3P) for all SAMHSA-hosted Web sites. It is the responsibility of the Web site Developers to make sure that the Web site being developed complies with these policies.

In order to collect data the following needs to be taken into consideration:

- OMB Clearance is required for any form, survey or database designed to collect information from Web site users.
- Section 208 Compliancy must be adhered to for all forms, surveys, and databases used for the purpose of collecting information. They also must be reviewed and approved by the SAMHSA Webmaster before going live.
- The SAMHSA Human-Readable Privacy Policies can be found at **http://www.samhsa.gov/privacy.aspx**.

Security and Restricted Access

Internet Security is a broad-based and complex topic. Therefore, this policy does not include significant guidelines on that subject. For any Internet Security issues, SAMHSA follows the HHS IT Service Center's Policy on Internet Security.

A password-restricted Web site or section of a Web site is allowed with approval from the Office of Communications and the Division of Management Systems—Information Technology. User ID's and passwords for this secured area are created by the IT Service Center. A meeting with the OC and DMS-IT will need to be conducted to work out all of the details of the requirement.

Exit Disclaimer

All links that point to non-government/military sites (.ORG, .COM, .NET, .EDU, .TV etc.) must have an **Exit Disclaimer** that appears in the user Web browser before being redirected to the new Web page. The text on the disclaimer message should say:

> "You are about to leave the SAMHSA Web site. SAMHSA provides links to other Internet sites as a service to its users, and is not responsible for the availability or content of these external sites. SAMHSA, its employees, and contractors do not endorse, warrant, or guarantee the products, services, or information described or offered at these other Internet sites. Any reference to a commercial product, process, or service is not an endorsement or recommendation by the SAMHSA, its employees, or contractors. For documents available from this server, the U.S. Government does not warrant or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed."

NOTE: Linking to external .gov and .mil Web sites is allowed without a disclaimer.

Required Footer Links

All SAMHSA Web sites must link to the following pages in the footer of every page:

- Home Page – the site home page
- Contact Us – a list of contacts for the program and the Web site
- Accessibility -- **http://www.samhsa.gov/about/508.aspx**
- Privacy Policy -- **http://www.samhsa.gov/privacy.aspx**
- FOIA -- **http://alt.samhsa.gov/foia/content/foia_main.html**
- Disclaimers -- **http://www.samhsa.gov/about/Disclaimer.aspx**
- SAMHSA -- **http://www.samhsa.gov/**
- HHS – **http://www.hhs.gov**
- FirstGov -- **http://www.firstgov.gov/**

Web Site Directory Structures (Onsite Hosting)

SAMHSA's Web site Directory Structures are managed by using the following Directory Structure layouts:

- Sites hosted on SAMHSA servers are placed under D:\Webs\<projectname> (no spaces).
- All databases used by Webs (where possible) are pulled from shared Web directories and placed in D:\databases.
- All images and other multimedia files must be stored in the /IMAGES folder located off the root directory of the Web site. Sub folders should be created topically (e.g., FLAGS) so that content creators can easily find images when creating a page.
- All Web log files will be pointed to D:\IISLogs. A text file will be placed in each subfolder, with the name of the corresponding Web.
- User-friendly folder and filenames are encouraged because they ultimately become the URL structure.

Naming Conventions for Web Site Files

Web page URL's are a direct reflection of the Web site's file and folder names (e.g., **http://intranet.samhsa.gov/budget/fy2005.aspx**). Having plain language folder names helps site visitors navigate the site, and relocate a previous page if they somehow get lost on the site, or have "jumped" to a location deep inside the Web site from a search engine or other source.

The naming conventions used for the SAMHSA Web site Files are as follows:

- No Spaces will be used in directory or filenames on public Web sites. Existing cases may remain at the discretion of the Webmaster.
- No more than one 'period' (.) may be used in a Web directory or filename (for example, about.us.html is not allowed. aboutus.html is OK). Files with more than one period are denied by **URLSCAN*** for security reasons.
- No files with the following extensions are permitted on SAMHSA public Web sites: (.exe, .com, .bat, .cmd, .ini, .log, .pol, .dat, .htw, .ida, .idq, .htr, .idc, .shtm, .shtml, .stm, .printer)
    1. **NOTE**: .shtm file includes should be renamed with an .html extension.
    2. All will be denied by **URLSCAN*** for security reasons.
    3. Executables as downloads may be made available in .zip format.
    4. Exceptions may be allowed in the future at the discretion of the Webmaster.

- None of the following URL sequences (i.e., sequence of characters typed into a browser address line) are permitted (all denied by **URLSCAN**):

.., ./ \ : % &

NOTE: *__URLSCAN__ is a Microsoft tool that sits at IIS's "front door" and examines HTTP requests to Web Servers, allowing or denying them based on a rule set. The rule set denies most common hacker scripts from reaching the Web Server and consuming valuable IIS resources.

NOTE: '&' has been allowed due to existing cases, but future sites must adhere to naming conventions set forth.

Permissible Browser Requests

The following are permissible 'HTTP Methods' (browser requests):

- GET, HEAD, POST, DEBUG, TRACE

WEBDAV extended HTTP Methods such as the following are denied by **URLSCAN**:

- PROPFIND, PROPPATCH, MKCOL, DELETE, PUT, COPY, MOVE, LOCK, UNLOCK, OPTIONS, SEARCH

Web Pages Must Link Back to the Home Page

To improve Web site usability, every Federal Web page must link back to its home page.

Implementation Guidance: Many people do not recognize that an agency's logo links to the home page. If an agency uses only a graphical link, it must contain text indicating that it links to the home page.

Page Flow

Maintaining a consistent page flow is an important way to optimize a Web site or Web-based application for search engines and optimize information dissemination for users.

Implementation Guidance: Good page flow can be achieved by following some simple rules—

- **Page Headings:** First, use <H1><H2><H3><H4> (heading) tags to denote headings. The higher the number, the smaller the page heading. Much like Microsoft Word and PowerPoint, some spiders rip pages apart while indexing them and create their own table of contents for the document, and use heading tags to pick out major chapters and start/stop points.

- **Site Architecture:** Page flow also refers to the architecture of the site, and how other pages are linked within. If the navigation is straight forward and clean, chances are good that spiders will have an easy time indexing the site and documents, and all of the pages desired will be followed by the spider.

Search Engine Usage

SAMHSA Web sites are not required to use a search engine. However if a Search Engine is to be implemented as a feature for a particular Web site (such as large sites, or sites where a search feature would significantly enhance the user experience), that site must point to the SAMHSA search engine located on **www.samhsa.gov** unless there is a compelling reason to build a separate customized search engine.

Customized search engines must obtain approval from the Government Project Officer and the SAMHSA Webmaster before development can begin.

An alternative approach to a search feature for smaller sites (though not required) is a Site Map, a clickable, text-based display of a Web site's hierarchy.

Search Engine Optimization

SAMHSA's Internet sites must be optimized for crawling by standard Internet search engines such as Google, Yahoo and Open Source directories. SAMHSA's Internet sites must read and implement the two sub-sections below:

Using a Robots.txt File
DOCTYPE, Character Sets, and META Tag

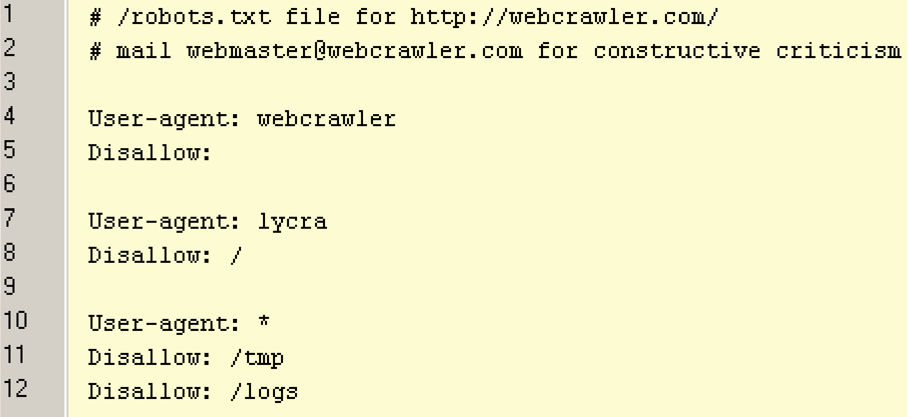
Using a Robots.txt File

All Internet Sites, and any other internal Web site that is to be included in the SAMHSA search engine, shall have a Robots.txt file stored in the top level (root) directory of the Web site.

The Robots.txt file optimizes Web application or Web sites for search engine crawls. By following the instructions in this file, search engines can be instructed to ignore archived files or obsolete information on the Web site. Developers can also include development files and related directories as part of the robots file if the robots.txt file indicates those files and folder should be ignored.

Implementation Guidance: Here is an example of a basic robots.txt file—

Figure 1 – Example robots.txt file



```
# /robots.txt file for http://webcrawler.com/
# mail webmaster@webcrawler.com for constructive criticism

User-agent: webcrawler
Disallow:

User-agent: lycra
Disallow: /

User-agent: *
Disallow: /tmp
Disallow: /logs
```

How to Disallow Folders or Files From Being Crawled

The robots.txt file above was built specifically to inform robots and spiders that there are certain directories on this server that the webmaster does not want parsed or indexed.

- The first two lines, starting with '#', specify a comment
- The first paragraph specifies that the robot called 'WebCrawler' has nothing disallowed: it may go anywhere.
- The second paragraph indicates that the robot called 'lycra' has all relative URLs starting with '/' disallowed. Because all relative URL's on a server start with '/', this means the entire site is closed off.
- The third paragraph indicates that all other robots should not visit URLs starting with /tmp or /log. Note the '*' is a special token, meaning "any other User-agent"; wildcard patterns or regular expressions cannot be used in either User-agent or Disallow lines.

How to Disallow A Specific Web Page from Being Crawled

To prevent a spider from indexing or caching a certain page, add the following line of code to the <HEAD> of the document:

```
<META NAME="ROBOTS" CONTENT="NOINDEX">
```

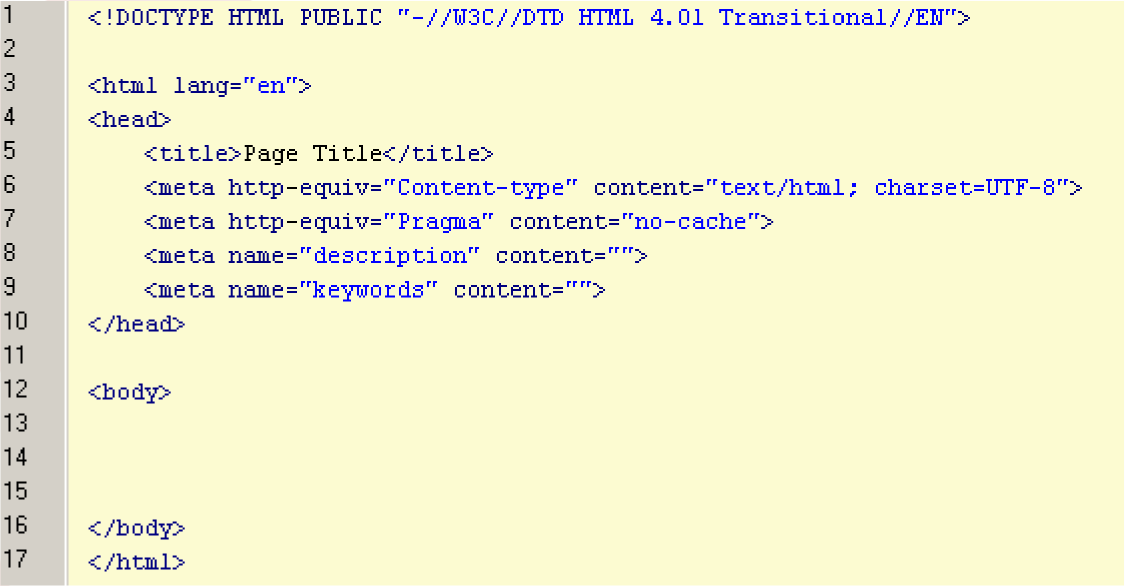
Additionally, to not have the links on that page followed (and then indexed) by the spider, add the following META tag to the <HEAD> of the document:

```
<META NAME="ROBOTS" CONTENT="NOFOLLOW">
```

DOCTYPE, Character Sets, and META tags

Another important thing to remember when building applications and Web sites that are going to be indexed in search engines is that the HTML needs to be well-formed, and also needs to include some basic tags & attributes. The term “well-formed” means that the HTML is valid (according to w3 standards), and contains no errors. See Figure 2 for an example of a perfect HTML 4.01 Transitional source (no content).

Figure 2 – Basic HTML layout



```
1   <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
2
3   <html lang="en">
4   <head>
5       <title>Page Title</title>
6       <meta http-equiv="Content-type" content="text/html; charset=UTF-8">
7       <meta http-equiv="Pragma" content="no-cache">
8       <meta name="description" content="">
9       <meta name="keywords" content="">
10  </head>
11
12  <body>
13
14
15
16  </body>
17  </html>
```

- On line 1 of the source code above is the DOCTYPE declaration. This is *extremely* important to include on **ALL** Web pages and application pages. A DOCTYPE informs browsers and validators what version of HTML (or XML, or XHTML) is being used, and must always appear as the very first line of code on the page.
- DOCTYPE declarations are essential to the proper rendering and functionality of Web documents and applications in standards compliant browsers, such as IE 6, Safari, Firefox, Mozilla, and Opera.
- Using an incomplete or outdated DOCTYPE – or no DOCTYPE at all – throws browsers into what is commonly called “Quirks” mode, where the browser assumes there is invalid or deprecated markup. In this setting, the browser will attempt to parse the page in backward-compatible fashion, rendering the styles as they might look in IE 4.0, reverting to a proprietary, browser-specific DOM. While some people may feel this is a good thing, it is actually a very bad thing. After all, one of the goals as a developer or designer is to make the content usable in as many formats as possible. To build an application or Web site that only works in IE, is cutting off the growing number of users who have

switched to Firefox or Opera, or are using a different OS, such as Mac OS X or Linux.

- Without having the correct DOCTYPE declaration, it is very possible that this page will be ignored or incorrectly indexed by search engines, especially Google.
- On line 3 of the code above, the standard <HTML> tag has the lang=”en” attribute attached to it. What this does is to declare to the browser that this page is in English, and should therefore be parsed in:
  - Only English-language fonts, and
  - Should be translated into English by text-readers and other browser add-ons.
- On line 5 is the <TITLE> tag. It is ESSENTIAL for search engine optimization that EVERY PAGE has a UNIQUE title. The <TITLE> tag is used by search engines on the results page. It is used to hyperlink to the page, and is the first thing the user sees when they parse the results. If the <TITLE> tag is not descriptive, or is the same for every page, the search results will be confusing.
- Another essential tag that should be on ALL pages is the <META> content-type declaration, which tells the browser which character set it should use to parse the pages. This is found on line 6 of the example above.
- SAMHSA uses the UTF-8 character set because it is the most universally recognized, and works very well with legacy systems. This exact tag should appear, as is, on all Web pages.
- On line 7 of the example, there is another <META> tag called the “Pragma” tag. This tag, while not essential, serves a very important function. It tells browsers and spiders NOT to cache the page in their history, so that every time they visit the site, they will get the newest content. Again, this tag is not essential, but it is very helpful in preventing people from caching data.
- Lines 8 and 9 are the basic META Description and Keyword tags. Much like the <TITLE> tag, each page needs to have a UNIQUE description and keywords, so that it can be indexed properly. The description should always be a quick summary of what that page shows, as well as keywords that are related to the content within the page.

For instance, if the page you are working on is for CMHS and relates to the latest grant information for psychiatric institutions, here’s the description and keywords to use:

```
<META name=”description” content=”2005 CMHS grant information for mental health institutions”>
<META name=”keywords” content=”samhsa, 2005, grant, mental, health, psychiatric, information”>
```

- The Meta elements “description” and “keyword” are part of the Dublin Core Metadata Element Set (version 1.1 as of 2/1/2005). The Dublin Core (as it is referred to in shorthand) are a set of Meta elements used to uniquely identify a document, its content, its creator(s), its format, and many other elements. There are a total of 15 elements in the Dublin Core. Those elements (and their definitions) are:

Element Name	**Description/Purpose**
Title	The name given to the document.
Creator	Author or person who maintains the document.
Subject or Keywords	Topic’s and relevant keywords related to the document.
Description	Short summary of the contents of the document.
Publisher	Name of the person who is responsible for making the document publicly viewable.
Contributor	A person or people who contributed to the creation of or the content within the document.
Date	Typically used for the date of last update to the document or its contents.
Resource Type	General category, genre, or aggregation level of the content.
Format	MIME type of the document (for Web – text/html commonly).
Resource Identifier	Typically indicates the URL (Universal Resource Locator), URI (Uniform Resource Identifier), or other unique string of characters/integers used to identify the document. ISBN is also an example.
Source	Similar to Resource Identifier. Typically used to identify the original source of the information contained within the document.
Language	Language which the document is published in. It is suggested that RFC 3066 (**http://www.ietf.org/rfc/rfc3066.txt**) should be used to code this element.
Relation	Reference information to a related resource
Coverage	Extent or scope of the content of the document, such as a time period, location, jurisdiction, or other similar identity.
Rights Management	Information about whether the document is covered by copyright or other intellectual property data.

- Typically, only a few of the Dublin Core elements are used for Web pages and applications. The most common are keyword, description, title, date, and publisher. Usage of these core elements should be determined on an organizational or departmental level.

Appendix A: References

HHS Web Records Guidance & Schedule, *in draft as of this writing*

HHS Policy for Internet Domain Names, **http://www.hhs.gov/policies/webpolicies/200501.html** (HHS-WEB-2005-01), 7/13/2005

SAMHSA's Identity Guide: Guidelines for the Use of HHS Logos, SAMHSA Symbols, and Program Icons, *not available online,* 6/2005

ITSC Security Program and Policy, *not available online,* 2005

HHS Information Quality Web Site: **http://aspe.hhs.gov/infoquality/Guidelines/index.shtml**, Apr 2004

OMB Memorandum M-05-04, Policies for Federal Agency Public Web sites, **http://www.whitehouse.gov/omb/memoranda/fy2005/m05-04.pdf**, 12/17/2004

HHS Information Quality Web Site, Section J, Substance Abuse and Mental Health Services Administration (SAMHSA): **http://aspe.hhs.gov/infoquality/Guidelines/SAMHSAinfo2.shtml**, Nov 2003

HHS Research-Based Web Design and Usability Guidelines, **http://usability.gov/pdfs/guidelines.html**, 9/2003

SAMHSA's Communications Planning and Clearance Process Guidelines, *not available online*, June 2003

Section 207 of the E-Government Act of 2002, **http://www.archives.gov/about/laws/egov-act-section-207.html**

Section 208 of the E-Government Act of 2002, **http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf**

OMB Information Quality Act, **http://www.whitehouse.gov/omb/fedreg/reproducible2.pdf**, 2002

Freedom of Information Act, **http://www.usdoj.gov/04foia/foiastat.htm**, amended 2002

Federal Records Act, **http://www.archives.gov/about/regulations/subchapter/b.html**, May 2002

HHS Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated to the Public, **http://aspe.hhs.gov/infoquality/Guidelines/index.shtml**, October 1, 2002

HHS IRM Policy on Usage of Persistent Cookies, **http://www.hhs.gov/read/irmpolicy/index.html** (HHS-IRM-2000-0009), 1/8/2001

Department of Justice guidance for Executive Order 13166, Improving Access to Services for People with Limited English Proficiency, **http://www.usdoj.gov/crt/cor/Pubs/lepqa.htm**, 8/11/2000

OMB Memorandum M-00-13, Privacy Policies and Data Collection on Federal Web Sites, **http://www.whitehouse.gov/omb/memoranda/m00-13.html**, 6/22/2000

OMB Memorandum M-99-18, Privacy Policies Federal Web Sites, **http://www.whitehouse.gov/omb/memoranda/m99-18.html** (and Attachment: Guidance and Model Language for Federal Web Site Privacy Policies, **http://www.whitehouse.gov/omb/memoranda/m99-18attach.html**), 6/2/1999

Section 508 of the Rehabilitation Act (29 U.S.C. 794d), **www.section508.gov**, 1998

OMB Circular A-130, Management of Federal Information Resources, **http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html**, rev. 2/2/1996

Paperwork Reduction Act of 1980, **http://www.archives.gov/federal-register/laws/paperwork-reduction/**, amended in 1995

Sections 501 and 504 of the Rehabilitation Act, **http://www.section508.gov/index.cfm?FuseAction=Content&ID=15**, 1973

Appendix B: Frequently Asked Questions (FAQs)

What is SAMHSA's Web Content Management Policy?

Several content management systems are being evaluated by the Division of Management Systems – Information Technology (DMS-IT) Team.

Does this Policy Apply to All SAMHSA Web Sites?

This policy only applies to SAMHSA-funded public Web sites. This includes in-house and externally hosted public Web sites funded through contracts, but does not include Web sites developed with funds from grants and cooperative agreements.

Are there any exceptions to this policy?

No. The SAMHSA Web policy applies to all SAMHSA components and Contractors providing public information via the official SAMHSA Web site. While the Agency recognizes the use of the Internet for many other functions besides dissemination of public information, this policy is limited to the Agency's information dissemination (or "publication") activities.

When does this policy take effect?

June 2006.

Why is this policy important?

SAMHSA Web pages are viewed by the public and employees as being the official position of the agency and have a high degree of visibility. It is imperative that Web content be overseen by management to ensure its quality, relevance to the agency's mission, and that it is delivered in a usable and accessible format.

Who is ultimately responsible for Web content?

The head of each SAMHSA organizational component is ultimately responsible for their content on the Agency's Web site and for its delivery. Therefore, all SAMHSA managers must adhere to the guidance and criteria established by the Office of Communications (OC) for the review and approval of Web content and its delivery.

Appendix C: Forms

HHS-524A

SAMHSA Web Site Certification Form

SAMHSA New Web Site Checklist

SAMHSA Checklist for Migrating Existing Web Sites to SAMHSA Servers

SAMHSA 508 Checklist for Developers and Contractors